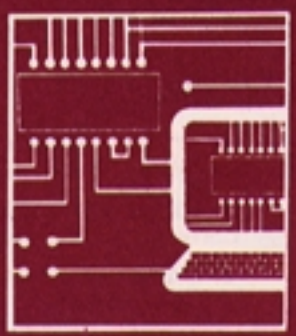
Federal Government Information Technology

Electronic Surveillance and Civil Liberties

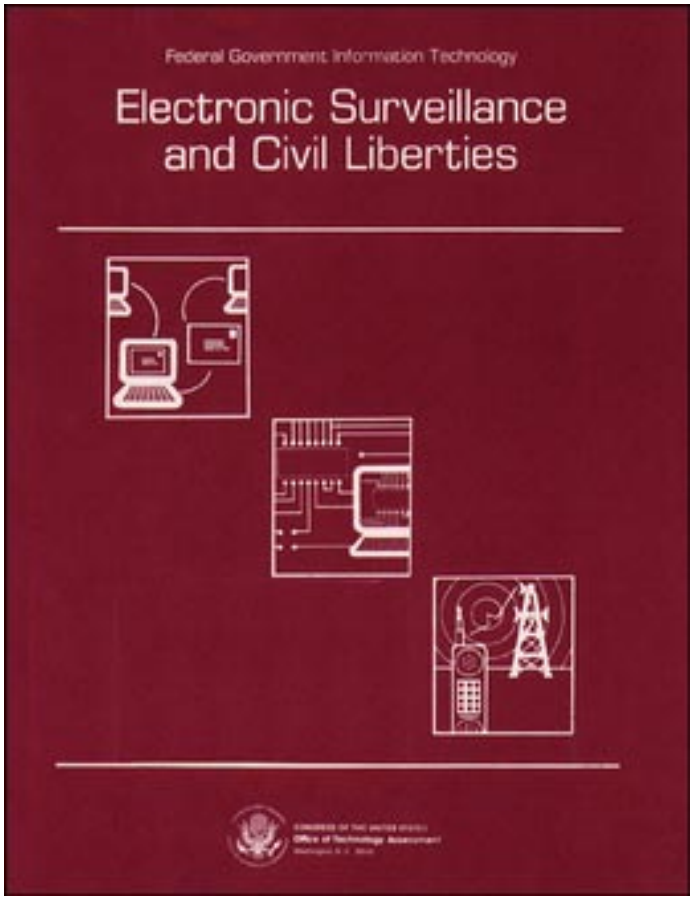


CONGRESS OF THE UNITED STATES
Office of Technology Assessment
Washington, D. C. 20510

Electronic Surveillance and Civil Liberties

October 1985

NTIS order #PB86-123239



Recommended Citation:

Federal Government Information Technology: Electronic Surveillance and Civil Liberties (Washington, DC: U.S. Congress, Office of Technology Assessment, OTA-CIT-293, October 1985).

Library of Congress Catalog Card Number 85-600609

For sale by the Superintendent of Documents
U.S. Government Printing Office, Washington, DC *20402*

Foreword

Public policy on the use of information technology to electronically monitor individual movements, actions, and communications has been based on a careful balancing of the civil liberty versus law enforcement or investigative interests. New technologies—such as data transmission, electronic mail, cellular and cordless telephones, and miniature cameras-have outstripped the existing statutory framework for balancing these interests.

The primary technical focus of this report is on technological developments in the basic communication and information infrastructure of the United States that present new or changed opportunities for and vulnerabilities to electronic surveillance, not on the details of specific surveillance devices. The primary policy focus is on domestic law enforcement and investigative applications, not on foreign intelligence and counterintelligence applications.

Thus, this report addresses four major areas: 1) technological developments relevant to electronic surveillance; 2) current and prospective Federal agency use of surveillance technologies; 3) the interaction of technology and public law in the area of electronic surveillance, with special attention to the balancing of civil liberty and investigative interests; and 4) policy options that warrant congressional consideration, including the amendment of existing public law to eliminate gaps and ambiguities in current legal protections.

Conducted at the request of the House Committee on the Judiciary, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, and the Senate Committee on Governmental Affairs, this report is one component of the OTA assessment of "Federal Government Information Technology: Congressional Oversight and Civil Liberties. Other topics covered in the assessment include: information technology management, planning, procurement, and security; computer crime; computer matching and privacy; electronic dissemination of Government information; and computer-based decision support, modeling, and Government foresight. These will be published under separate cover.

In preparing this report on electronic surveillance, OTA has drawn on working papers developed by OTA staff and contractors, the comments of participants at an OTA workshop on this topic, and the results of an OTA Federal Agency Data Request that was completed by over 140 agency components. The draft of this report was reviewed by the OTA project advisory panel, officials from the U.S. Department of Justice, and a broad spectrum of interested individuals from the governmental, academic, private industry, and civil liberty communities.

OTA appreciates the participation of the advisory panelists, workshop participants, external reviewers, Federal agency officials, and others who helped bring this report to fruition. The report itself, however, is solely the responsibility of OTA, not of those who so ably advised and assisted us in its preparation.

JOHN H. GIBBONS
Director

Electronic Surveillance and Civil Liberties Advisory Panel

Theodore J. Lowi, *Chairman*
Professor of Political Science, Cornell University

Arthur G. Anderson
IBM Corp. (Ret.)

Jerry J. Berman
Legislative Counsel
American Civil Liberties Union

R. H. Bogumil
Past President
IEEE Society on Social Implications of Technology

James W. Carey
Dean, College of Communications
University of Illinois

Melvin Day
Vice President
Research Publications

Joseph W. Duncan
Corporate Economist
The Dun & Bradstreet Corp.

William H. Dutton
Associate Professor of Communications and Public Administration
Annenberg School of Communications
University of Southern California

David H. Flaherty
Professor of History and Law
University of Western Ontario

Carl Hammer
Sperry Corp. (Ret.)

Starr Roxanne Hiltz
Professor of Sociology
Upsala College

John C. Lautsch
Chairman, Computer Law Division
American Bar Association

Edward F. Madigan
Office of State Finance
State of Oklahoma

Marilyn Gell Mason
Director
Atlanta Public Library

William Joe Skinner
Corporate Vice President
Electronic Data Systems Corp.

Terril J. Steichen
President
New Perspectives Group, Ltd.

George B. Trubow
Director, Center for Information Technology and Privacy Law
The John Marshall Law School

Susan Welch
Professor and Chairperson
Department of Political Science
University of Nebraska

Alan F. Westin
Professor of Public Law and Government
Columbia University

Langdon Winner
Associate Professor of Political Science
Rensselaer Polytechnic Institute

Congressional Agency Participants

Robert L. Chartrand
Senior Specialist
Congressional Research Service

Robert D. Harris
Deputy Assistant Director for Budget Analysis
Congressional Budget Office

Kenneth W. Hunter
Senior Associate Director for Program Information
U.S. General Accounting Office

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by these advisory panel members. The views expressed in this OTA report, however, are the sole responsibility of the Office of Technology Assessment.

OTA Electronic Surveillance and Civil Liberties Project Staff

John Andelin, *Assistant Director, OTA*
Science, Information, and Natural Resources Division

Frederick W. Weingarten, *Communication and Information Technologies*
Program Manager

Project Staff

Fred B. Wood, *Project Director*

Jean E. Smith, *Assistant Project Director*

Priscilla M. Regan, *Principal Author and Analyst*

Jim Dray, *Research Analyst*

Jennifer Nelson, *Research Assistant*

Administrative Staff

Elizabeth A. Emanuel, *Administrative Assistant*

Shirley Gayheart, *Secretary*

Audrey Newman, *Secretary*

Renee Lloyd, *Secretary*

Patricia Keville, *Clerical Assistant*

Contractor

Herman Schwartz, *The American University*

OTA Electronic Surveillance and Civil Liberties Workshop

Stanley S. Arkin
Attorney

Peter Benitez
New York County District Attorney's Office

Kier Boyd
Deputy Assistant Director
Technical Services Division
Federal Bureau of Investigation

James C. Carr
U.S. Magistrate

Floyd Clarke
Deputy Assistant Director
Criminal Division
Federal Bureau of Investigation

Russell Cestare
Chief of Liaison and Communication
Financial Investigations Division
U.S. Customs Service

Ronald C. Farm
Chief, Counterintelligence Operations
U.S. Department of the Army

Richard Gerstein
Partner
Bailey, Gerstein, Rashkind & Dresnick

Morton H. Halperin
Director
American Civil Liberties Union

Frederick D. Hess
Head, Office of Enforcement Operations
Criminal Division
U.S. Department of Justice

Mary Lawton
Counsel, Office of Intelligence and Policy Review
U.S. Department of Justice

Frederick B. Lothrop
Analyst/Project Manager
PSC, Inc.

Paul Lyon
Chief of Special Operations
Bureau of Alcohol, Tobacco and Firearms
U.S. Department of the Treasury

Gary Marx
Professor, Department of Urban Studies and Planning
Massachusetts Institute of Technology

Ronald S. Plesser
Attorney
Blum, Nash & Railsback

Christopher Pyle
Professor, Political Science Department
Mount Holyoke College

James B. Rule
Professor, Department of Sociology
State University of New York at Stony Brook

Herman Schwartz
Professor of Law
The American University

L. Britt Snider
Director, Counterintelligence and Security Policy
Office of the Secretary of Defense

Other Reviewers

Michael Cavanagh
Electronic Mail Association

Charles Miller
American Telephone & Telegraph Co.

David Peyton
Information Industry Association

Barbara Philips
Telocator Network of America

Harold Relyea
Congressional Research Service

Contents

Chapter		Page
1.	Summary	3
2.	Introduction and Overview	9
	Summary	9
	Introduction	11
	Background	12
	Technology and Use	12
	Policy	15
	Findings and Policy Implications	21
	Appendix 2A: Key Supreme Court Decisions on Electronic Surveillance	24
	Appendix 2B: Key Statutes Relevant to Electronic Surveillance	25
3.	Telephone Surveillance	29
	Summary	29
	Introduction	30
	Background	31
	Findings and Policy Implications	34
4.	Electronic Mail Surveillance	45
	Summary	45
	Introduction	45
	Background	46
	Findings and Policy Implications	48
5.	Other Surveillance Issues	55
	Summary	55
	Electronic Physical Surveillance	55
	Electronic Visual Surveillance	55
	Data Base Surveillance	56
	Part I: Electronic Physical Surveillance	57
	Introduction	57
	Background	57
	Findings and Policy Implications	59
	Part II: Electronic Visual Surveillance	62
	Introduction	62
	Background	63
	Findings and Policy Implications	64
	Part III: DataBase Surveillance	67
	Introduction	67
	Background	68
	Findings and Policy Implications	70

List of Tables

Table No.		Page
1.	Categories of Surveillance Technology	13
2.	Categories of Behavior Subject to Electronic Surveillance	13
3.	Top Fifteen Agency Components Using Electronic Surveillance Technology	14
4.	Electronic Surveillance Technology: Current and Planned Agency Use	15
5.	Agency Components Indicating the Largest Projected Use of Electronic Surveillance Technology	15
6.	Dimensions for Balancing Civil Liberty Interest v. Government Investigative Interest	22
7.	Treasuray Enforcement Communication System/Border Enforcement System Users	69
8	Source of Treasury Enforcement Communication System/Border Enforcement System Records.	69
9	Selected INS Computerized Record Systems	70

Chapter 1
Summary

Chapter 1

Summary

In the last 20 years, there has been a virtual revolution in the technology relevant to electronic surveillance. Advances in electronics, semiconductors, computers, imaging, data bases, and related technologies have greatly increased the technical options for surveillance activities. Closed circuit television, electronic beepers and sensors, and advanced pen registers are being used to monitor many aspects of individual behavior. Additionally, new electronic technologies in use by individuals, such as cordless phones, electronic mail, and pagers, can be easily monitored for investigative, competitive, or personal reasons.

The existing statutory framework and judicial interpretations thereof do not adequately cover new electronic surveillance applications. The fourth amendment–which protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures' '—was written at a time when people conducted their affairs in a simple, direct, and personalized fashion. Telephones, credit cards, computers, and cameras did not exist. Although the principle of the fourth amendment is timeless, its application has not kept abreast of current technologies.

The major public law addressing electronic surveillance is Title III of the Omnibus Crime Control and Safe Streets Act of 1968 which was designed to protect the privacy of wire and oral communications. At the time Congress passed this act, electronic surveillance was limited primarily to simple telephone taps and concealed microphones (bugs). Since then, the basic communications infrastructure in the United States has been in rapid technological change. For example, satellite communication systems and digital switching and transmission technology are becoming pervasive, along with other easily intercepted technical applications such as cellular mobile radio, cordless telephones, electronic mail, computer conferencing, and electronic bulletin boards. Continued advances in computer-communications technology such as the Integrated Services Digital Network (ISDN), now close to implementation, are likely to present additional new opportunities for electronic surveillance.[1]

The law has not kept pace with these technological changes. The courts have, on several occasions, asked Congress to give guidance. Most recently, U.S. Circuit Court Judge Richard Posner, in a case involving the use of video surveillance in a law enforcement investigation, said:

> . . . we would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope . . . judges are not authorized to amend statutes even to bring them up to date.

In legislating the appropriate uses of electronic surveillance, Congress attempts to strike a balance between civil liberties—especially those embodied in the first, fourth, and fifth amendments to the U.S. Constitution–and the needs of domestic law enforcement and investigative authorities for electronic surveillance in fighting crime, particularly white-collar and organized crime, and generally for drug, gambling, and racketeering investigations.'

Law enforcement and investigative agencies, at least at the Federal level, are making significant use of electronic surveillance techniques and are planning to use many new techniques. Based on a review of available reports

[1]ISDN permits the transmission of voice, video, and data signals as needed over a common multi-purpose communications network,

[2]Note: This study did not review technology or policy issues concerning foreign intelligence and counterintelligence applications of electronic surveillance.

and the results of its Federal Agency Data Request,[3] OTA found that:

- The number of Federal court-approved bugs and wiretaps in 1984 was the highest ever.
- About 25 percent of Federal agency components responding (35 out of 142) indicated some current and/or planned use of various electronic surveillance technologies, including, but not limited to, the following:
  —closed circuit television (29 agencies);
  —night vision systems (22);
  —miniature transmitters (21);
  —electronic beepers and sensors (15);
  —telephone taps, recorders, and pen registers (14);
  —computer usage monitoring (6);
  —electronic mail monitoring or interception (6);
  —cellular radio interception (5);
  –pattern recognition systems (4); and
  —satellite interception (4).
- About 25 percent of Federal agency components responding (36 out of 142) report use of computerized record systems for law enforcement, investigative, or intelligence purposes:
  —agencies reported a total of 85 computerized systems with, collectively, about 288 million records on 114 million persons;[4]
  —examples of four such systems that could be used in part for data base surveillance purposes are the:
    1. National Crime Information Center (FBI),
    2. Treasury Enforcement Communications System (Treasury),
    3. Anti-Smuggling Information System (Immigration and Naturalization Service–INS), and
    4. National Automated Immigration Lookout System (INS).
  —none of the 85 system operators provided the requested statistics on record quality (completeness and accuracy). Most do not maintain such statistics.

After conducting a review of the technology and policy history of electronic surveillance, OTA found that:

- The contents of phone conversations that are transmitted in digital form or calls made on cellular or cordless phones are not clearly protected by existing statutes.
- Data communications between computers and digital transmission of video and graphic images are not protected by existing statutes.
- There are several stages at which the contents of electronic mail messages could be intercepted: 1) at the terminal or in the electronic files of the sender, 2) while being communicated, 3) in the electronic mailbox of the receiver, 4) when printed into hardcopy, and 5) when retained in the files of the electronic mail company or provider for administrative purposes. Existing law offers little or no protection at most of these stages.
- Legislated policy on electronic physical surveillance (e.g., pagers and beepers) and electronic visual surveillance (e.g., closed circuit TV and concealed cameras) is ambiguous or nonexistent.
- Legislated policy on data base surveillance (e.g., monitoring of transactions on computerized record systems and data communication linkages) is unclear.
- There is no immediate technological answer to protection against most electronic surveillance, although there are emerging techniques to protect communication systems from misuse or eavesdropping (e.g., low-cost data encryption).[5]

OTA identified a range of policy options for congressional consideration:

- Congress could do nothing and leave policymaking up to the development of case

[3]The data request was sent to all major components within the 13 cabinet-level agencies and to 20 selected independent agencies. Due to the unclassified focus of this study, two Department of Defense components–the National Security Agency and Defense Intelligence Agency–along with the Central Intelligence Agency were excluded from the data request.

[4]Extent of multiple records on the same person is unknown.

[5]Technical options are being addressed in a separate OTA study on "New Communications Technology: Implications for Privacy and Security," expected to be published in winter 1986/87.

law and administrative discretion. However, this would lead to continued uncertainty and confusion regarding the privacy accorded phone calls, electronic mail, data communication, and the like, and ignores judicial requests for clarification in areas such as electronic visual surveillance.

- Congress could bring new electronic technologies and services clearly within the purview of Title III of the Omnibus Crime Control and Safe Streets Act, for example by:
  - –treating all telephone calls similarly with respect to the extent of protection against unauthorized interception, whether analog or digital, cellular or cordless, radio or wire;
  - –legislating statutory protections against unauthorized interception of data communication;
  - –legislating a level of protection across all stages of the electronic mail process so that electronic mail is afforded the same degree of protection as is presently provided for conventional first class mail;
  - —subjecting electronic visual surveillance to a standard of protection similar to or even higher than that which currently exists under Title 111 for bugging and wiretapping.
- Congress also could set up new mechanisms for control and oversight of Federal data base surveillance, for example by:
  - —requiring congressional approval of specific Federal data base surveillance applications (e.g., by statutory amendment or approval of House and Senate authorizing committees);
  - —establishing a data protection board to administer and oversee general statutory standards for creating and using data bases for purposes of surveillance.
- Congress also could amend the Computer Fraud and Abuse Act of 1984 to cover interstate computer crime.
  - —This option, not detailed here, could provide additional legal protection against unauthorized penetration (whether for surveillance or other reasons, e.g., theft or fraud) of computer systems.[G]

Chapters 2 through 5 of this report provide technical and policy analyses relevant to proposed legislation on electronic surveillance and civil liberties, such as the "Electronic Communications Privacy Act of 1985' and the "Video Surveillance Act of 1985.'"

[G]See the computer crime chapter of the forthcoming OTA report on "Federal Government Information Technology: Key Trends and Policy Issues" for discussion.

'H.R. 3378 introduced by Rep. Robert Kastenmeier and S. 1667 introduced by Sen. Patrick Leahy. See U.S. Congress, House of Representatives, *Congressional Record,* Extension of Remarks, Sept. 19, 1985, p. E-4 128; and U.S. Congress, Senate, *Congressional Record,* Sept. 19, 1985, p. S-11 795.

'11. R. 3455 introduced by Representative Kastenmeier. See U.S. Congress, House of Representatives, *Congressional Record,* Extension of Remarks, Sept. 30, 1985, p. I+; -4269.

Chapter 2

Introduction and Overview

Chapter 2
Introduction and Overview

SUMMARY

Electronic surveillance is the epitome of the two-edged sword of technology for many Americans. Public opinion polls evidence considerable concern about possible excessive and abusive use of electronic surveillance by the Government (and others), and show support for strong safeguards and protections to tightly control the use of such technology. But, at the same time, the public is concerned about crime—especially violent crime—and supports the appropriate use of technology to combat and prevent crime and bring offenders to justice. [1]

Until the past 10 years or so, the balancing of these concerns was relatively straightforward from a technological perspective. Electronic surveillance was limited primarily to audio surveillance devices such as telephone taps and concealed microphones ("bugs"). Now, however, technological developments have significantly expanded the range of electronic surveillance options. These include miniaturized transmitters for audio surveillance, lightweight compact television cameras for video surveillance, improved night vision cameras and viewing devices, and a rapidly growing array of computer-based surveillance techniques. In addition, most forms of electronic communication—whether via wire, coaxial cable, microwave, satellite, or even fiber optics—can be monitored if one has the time, money, and technical expertise. Encryption–the only technological countermeasure thought at this time to be generally effective—is still too expensive and cumbersome for widespread application, although costs are declining and ease of use is improving.

The primary purpose of electronic surveillance is to monitor the behavior of individuals, including individual movements, actions, communications, emotions, and/or various combinations thereof, as well as the movement of property or objects. Some uses of electronic surveillance devices may infringe on the protections afforded by the first, fourth, and fifth amendments to the U.S. Constitution and various public laws.

This chapter surveys the Federal Government's use of electronic surveillance and outlines a framework for the analysis of electronic surveillance issues.

Based on a review of available reports and the results of its Federal Agency Data Request, OTA found that:

- The extent of use of electronic surveillance by the private sector is unknown.
- The number of Federal and State court-approved wiretaps and bugs reported in 1984 was the highest since 1973.
- The number of Federal court-approved bugs and wiretaps in 1984 was the highest ever.
- According to early reports, an average of about 25 percent of intercepted communications in 1984 were reported to be incriminating in nature, with 2,393 persons arrested as a result of electronic surveillance.
- About 25 percent of Federal agency components responding to the OTA Federal Data Request indicated some use of electronic surveillance. [2]

[1] See Alan F. Westin, "Public and Group Attitudes Toward Information Policies and Boundaries for Criminal Justice," in U.S. Department of Justice, Bureau of Justice Statistics, *Information Policy and Crime Control Strategies,* Proceedings of a BJS/SEARCH Conference, July 1984, pp. 32-46; and William H. Dutton and Robert G. Meadow, "Public Perspectives on Government Information Technology: A Review of Survey Research on Privacy, Civil Liberties, and the Democratic Process," OTA contractor report, January 1985.

[2] Due to the unclassified focus of this study, two Department of Defense components—the National Security Agency and Defense Intelligence Agency-along with the Central Intelligence Agency were excluded from the data request.

53.548 O - 85 - 2 : QL 3

– Federal agency use is concentrated in components of the Departments of Justice, Treasury, Defense, Agriculture, and Interior.
— The Drug Enforcement Administration and Federal Bureau of Investigation (Justice), U.S. Customs Service (Treasury), and Air Force Office of Special Investigations (Defense) use the greatest number of different types of electronic surveillance technologies.
— The FBI, which currently uses nine different types of surveillance technologies, has plans to use eight additional types of technologies.

A thorough review of the technology and policy history of electronic surveillance led OTA to conclude that:

- The existing statutory framework and judicial interpretations thereof do not adequately cover new and emerging electronic surveillance technologies. Indeed, the courts have asked Congress for guidance on the new technologies.
- There is no immediate technological answer to protection against most electronic surveillance, although there are emerging techniques to protect communication systems from misuse or eavesdropping (e.g., low-cost data encryption).
- Despite a lack of coordination in electronic surveillance policymaking among the three branches of Government and the ad hoc nature of that policy, there are seven general components that are found in existing policies, be they legislative, executive, or judicial:
  1. a way of checking on the discretion of the Government agent in the field;
  2. a listing of the crimes and circumstances for which a particular type of electronic surveillance is considered appropriate;
  3. a standard to indicate at what stage in an investigation the use of a particular surveillance technique is appropriate;
  4. a justification for the need to use a particular surveillance technique;
  5. an account of how the scope of the surveillance will be minimized;
  6. a requirement to give notice after the fact to the subject of the surveillance; and
  7. remedies and sanctions, including a statutory exclusionary rule or a civil remedy.
- In setting electronic surveillance policy, Congress, the executive branch, and the courts, implicitly or explicitly, balance the societal interest in maintaining civil liberties protections for the individual against the societal interest in successful Government investigations. Based on an evaluation of previous policy formulation, policymakers, more or less consciously, have looked to certain dimensions in determining this balance.
- In determining the civil liberty interest with respect to electronic surveillance, policymakers look to five dimensions—the nature of information, the nature of the place or communication, the scope of the surveillance, the surreptitiousness of surveillance, and the pre-electronic analogy of the surveillance technique or device.
- In determining the Government's interest, policymakers have used three dimensions to evaluate the need for using an electronic surveillance technique or device-the purpose of the investigation, the degree of individualized suspicion, and the effectiveness of the electronic device as an investigatory tool compared to nonelectronic options.

This policy framework is applied in the following chapters to specific types of electronic surveillance technology.

INTRODUCTION

The capabilities for surveillance-the observation and monitoring of individual or group behavior including communication-are greatly expanded and enhanced with the use of technological devices. For example, technology makes it more efficient and less conspicuous to track movements, to hear conversations, to know the details of financial and other personal transactions, and to combine information from diverse sources into a composite file.

New surveillance tools are technically more difficult to detect, of higher reliability and sensitivity, speedier in processing time, less costly, more flexible and adaptable, and easier to conceal because of miniaturization and remote control. Current R&D will produce devices with increased surveillance capabilities, e.g., computer speech recognition and speaker identification, fiber optics, and expert systems.

Many electronic devices are currently available for monitoring individual or group behavior. For example, phone conversations might be overheard, records of phone numbers dialed might be accessed, movements at home and in the workplace might be video-recorded, and movements outside the home or workplace, even in the dark, could be observed. In addition, bank and credit records could be examined electronically to determine financial habits and general movements, and conversations in a public place could be recorded by a parabolic microphone. Further, it is possible that actions might be evaluated by computer to determine whether they match any profiles or have a pattern, that electronic mail communication might be accessed and read, that the movements of physical objects such as a car might be tracked by a beeper, and that a new friend or local taxi driver might be wired for sound.

From a law enforcement and investigative standpoint, the potential benefits offered through new electronic technologies may be substantial-e. g., the development of more accurate and complete information on suspects, the possible reduction in time and manpower required for case investigation, and the expansion of the options for preventing and deterring crimes. From a societal perspective, the possible benefits are also important–including the potential to increase one's sense of physical security in the home and on the streets, improve the capability to know when someone is in need of assistance, strengthen efforts to prevent the sale of illegal substances, and enhance the protection of citizens and Government officials from terrorist actions.

However, while providing increased security, the use of sophisticated technologies for surveillance purposes also presents possible dangers to society.[1] Over time, the cumulative effect of widespread surveillance for law enforcement, intelligence, or other investigatory purposes could change the climate and fabric of society in fundamental ways. For example, how will hotlines that encourage people to anonymously report potentially damaging information and one-party consent to the monitoring of conversations affect the level of trust in our society? Will private space and anonymity be preserved when individuals increasingly must make private information widely available, e.g., to banks, medical clinics, and credit agencies, in order to carry on everyday activities? How will informality and spontaneity in communications and behavior be affected as more personal activities are "on the record' or "in view?"

But most importantly for the purposes of this study, the use of electronic surveillance devices may infringe on the protections afforded in the first amendment (freedom of speech and press, and the right to peaceably assemble and to petition the Government for a redress of grievances), fourth amendment (unreasonable searches and seizures), and fifth amendment (protection against self-incrimination). The use of such devices may also conflict with procedural and substantive protections in specific statutes, e.g., Title III of the

[1]Gary T. Marx, "The New Surveillance," *Technology Review*, vol. 88, No. 4, May June 1985, pp. 42-48.

1968 Omnibus Crime Control and Safe Streets Act, the Privacy Act of 1974, the Foreign Intelligence Surveillance Act of 1978, the Electronic Funds Transfer Act of 1978, and the Cable Communications Policy Act of 1984.

Many innovations in electronic surveillance technology have outstripped constitutional and statutory protections, leaving areas in which there is currently no legal protection against, or controls on the use of, new surveillance devices. In 1928, Justice Louis Brandeis, in his dissenting opinion in Olmstead v. *United States,* warned that:

> Subtler and more far reaching means of invading privacy have become available to the Government . . . the progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government. without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[4]

Although use of some surveillance techniques requires a court order, many do not require any authorized approval and some are not even covered by judicial interpretation of the fourth amendment prohibition on unreasonable searches and seizures. Additionally, the privacy and procedural rights of those subject to surveillance may also be violated, since their activities may be monitored even though no criminal suspicion has attached to them. Finally, given the unobtrusive nature of surveillance activities, it may be difficult to detect when one's rights have been violated.

The use of electronic surveillance devices may result in more efficient law enforcement. Their use may be required in part by the use of more evasive and sophisticated devices by those suspected of engaging in criminal activities. Yet, the cumulative impact of the increased use of surveillance, with or without a court order, is an important consideration for any society that prides itself on limited government and individual freedom.

The key policy issue is to determine the appropriate balance between the civil liberty interests and the intelligence, law enforcement, or other governmental interests involved. In some circumstances, the law enforcement interest will be great enough to outweigh the civil liberty interest. In other circumstances, the reverse will be the case. Policy, be it judicial, legislative, or administrative, seeks to define the parameters for this balancing process.

James Madison addressed this basic dilemma of democratic governments in *Federalist #51:*

> If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the Government to control the governed; and in the next place, oblige it to control itself.

[4] *Olmstead v. United States,* 277 U.S. **438, 473-474** (1928).

BACKGROUND

Technology and Use

For much of the 20th century, electronic surveillance technology was limited primarily to audio surveillance devices such as telephone taps and concealed microphones ("bugs"). In the late 1960s, however, technological developments began to significantly expand the range of electronic surveillance options. These included miniaturized transmitters for audio surveillance, lightweight compact television cameras for video surveillance, improved night vision cameras and viewing devices, and the first computer-based surveillance techniques. In the 1970s, congressional attention focused on electronic surveillance, partly due to the use of surveillance technologies during the Civil Rights Movement and in Watergate, but also

due to a perception of a growing application of such technology in various sectors of society. Table 1 presents a list of categories and types of surveillance technology as developed by the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary in 1976.

The primary purpose of electronic surveillance technology is to monitor the behavior of individuals. As illustrated in table 2, electronic devices can be used to monitor individual movements, actions, communications, emotions, and/or various combinations thereof.

It appears that many of the electronic surveillance technologies identified in table 1 were not widely used in 1976, partly because the underlying media of communication (e.g., electronic mail and cellular radio) were not in wide service. However, there is no authoritative information on the full extent of their use.

Table 1 .–Categories of Surveillance Technology

1. Electronic *eavesdropping technology* (audio survei l lance)
   - . radiating devices and receivers (e g , miniaturized transmitters)
   - . nonradiating devices (e g., wired surveillance systems, Including telephone taps and concealed microphones)
   - • tape recorders
2. Optical/imaging technology (visual surveillance)
   - • photographic techniques
   - • television (closed circuit and cable)
   - . night vision devices (use image intensifier to view objects under low light)
   - • satellite based
3. Computers and *re/ated technologies* (data surveillance)
   - • microcomputers —decentralization of machines and distributed processing
   - Ž computer networks
   - • software (e. g., expert systems)
   - • pattern recognition systems
4. *Sensor technology*
   - • magnetic sensors
   - • seismic sensors
   - . ınfrared sensors
   - • strain sensors
   - • electromagnetic sensors
5. Other devices and technologies
   - • citizen band radios
   - . vehicle location systems
   - • machine-readable magnetic strips
   - •s polygraph
   - • voice stress analyzer
   - • voice recognition
   - • laser interception
   - Ž cellular radio

SOURCE Based on the framework developed by the Senate Judiciary Committee s Subcommittee on Constitut ıon al Rıg hts ınits report *Surveillance Technology – 1976* seepp 29 37)

Table 2.—Categories of Behavior Subject to Electronic Surveillance

1. Movements—where someone Is. Individuals can be tracked electronically via beepers as well as by monitoring computerized transactional accounts in real time
2. Actions-what someone is doing or has done. Electronic devices to monitor action include: monitoring of keystrokes o n computer terminals, monitoring of telephone numbers called with pen registers, cable TV monitoring, monitoring of financial and commercial computerized accounts. and accessing computerlzed law enforcement or investlgatory systems.
3. Communications—what someone is saying or writing. and hearing or receiving. Two-way electronic communications can be intercepted whether the means be analog or digi - tal communication via wired telephones, communication via cordless or cellular phones, or digital electronic mail communication. Two-way nonelectronic communication can be intercepted via a variety of m microphone devices and other transmitters.
4. *Actions* and communications —the details of what some one is doing or saying Electronic visual surveillance, generally accompanied by audio surveillance, can monitor the actions and communications of individuals i n both private and public places, in daylight or darkness
5. Emotions —the psychological and physiological reactions to circumstances. Polygraph testing, voice stress analyzers, breath analyzers, and brain wave analyzers attempt to determine an Individual's reactions.

SOURCE Offi ce of Technology Assessn ent

In the private sector (not involving the Government), the FBI notes that the number of reported incidents of illegal interception of private sector communications declined from 524 in 1981 to 392 in 1984.[5] However, it is likely that only a small fraction of total incidents occurring are reported, and it is probable that many forms of private sector electronic surveillance go undetected, and if detected, go unreported.

Statistics on Government use of some electronic surveillance techniques, primarily telephone wiretaps and hidden microphones, are collected and published by the Administrative Office of the U.S. Courts. The April 1985 report indicates that in 1984, Federal and State judges approved 801 out of 802 requests for electronic surveillance-289 by Federal judges

[5] John Horgan, "Thwarting the Information Thieves," *IEEE Spectrum*, July 1985, p. 32, which cites the source as FBI spokesperson William Carter.

and 512 by State judges. The 1984 combined total of 801 was the highest since 1973. The 1984 Federal total of 289 was the highest ever, with the prior peak year being 1971. Overall, the number of State electronic surveillance orders has slowly declined since 1973, while Federal surveillance orders declined from 1971 to 1977, remained about constant from 1977 to 1980, and increased from 1981 to the present. The number of electronic interceptions authorized by Federal courts in 1984 is almost triple the 1981 level.[6]

In general, the reported electronic surveillance is used primarily in narcotics and gambling cases; in 1974 gambling was first and narcotics second, and in 1984 the order was reversed. The reported cost of electronic surveillance has increased dramatically, from about $8,000 each in 1974 to about $45,000 each in 1984. An average of about 25 percent of intercepted communications in 1984 was reported to be incriminating in nature, with 2,393 persons arrested as a result of electronic surveillance and about 27 percent of those convicted.[7] The figures for arrests and convictions are necessarily incomplete because of the time involved in concluding a Federal criminal case.

Because of the general lack of information on Federal use of electronic surveillance, questions on this topic were included in the OTA Federal Agency Data Request sent to the 13 cabinet-level departments and 20 selected independent agencies. Of 142 agency components responding, 35 or about 25 percent reported some current use of electronic surveillance technology for monitoring the movement, activity, conversation, or information pertaining to individuals or agencies in which the agency has an investigative, law enforcement, and/or intelligence interest. Of these 35 agency components, the top 15 agencies reporting use of the largest number of electronic surveillance technologies are listed in table 3. (Note that the Central Intelligence Agency, National Security Agency, and Defense Intelligence Agency were excluded from the data request.)

Table 3.—Top Fifteen Agency Components Using Electronic Surveillance Technology

Agency[a]	Number of technologies currently used
Drug Enforcement Administration (DOJ)	10
Federal Bureau of Investigation (DOJ)	9
U.S. Customs Service (Treasury)	9
U.S. Air Force (DOD)	9
National Park Service (DOI)	8
Internal Revenue Service (Treasury)	7
Criminal Division (DOJ)	7
U.S. Forest Service (USDA)	7
Inspector General (USDA)	7
Agricultural Stabilization and Conservation Service (USDA)	7
U.S. Army (DOD)	6
Fish and Wildlife Service (DOI)	6
U.S. Marshals Service (DOJ)	6
U.S. Mint (Treasury)	6
Bureau of Alcohol, Tobacco and Firearms (Treasury)	6

[a]The Central Intelligence Agency National Security Agency, and Defense Intelligence Agency were excluded due to the unclassified focus of this study

SOURCE Office of Technology Assessment

Use of specific technologies varied widely, with use of closed circuit television, night vision systems, radio scanners, and miniature transmitters indicated by many agencies that conduct electronic surveillance, and use of telephone taps, vehicle location systems (e.g., beepers), sensors, and pen registers indicated by a smaller but still significant number of agencies. The other technologies are used by relatively few or very few agencies. Actual results of the OTA Data Request are summarized in table 4. Out of the 35 agencies indicating some electronic surveillance activity, the FBI and DOD Inspector General's Office indicated the largest planned expansion in use of electronic surveillance technologies (see table 5).

The technical literature suggests that most forms of electronic communication can be intercepted, although it may be difficult and costly. The cost of equipment needed to intercept microwave telephone circuits has been estimated at about $40,000, but it can be done relatively easily and without the awareness of

[6]Administrative Office of the United States Courts, *Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications*, for Calendar 1984, Washington, DC, April 1985, pp. 3, 6, 21.

[7]Ibid., pp. 6, 7, 21.

Table4 .—Electronic Surveillance Technology: Current and Planned Agency Use

Technology	Number of agency components reporting: Current use	Planned use	Total
Closed circuit television	25	4	29
Night vision systems	21	1	22
Miniature transmitters	19	2	21
Radio receivers (scanners)	19	1	20
Vehicle location systems (e. g., electronic beepers)	13	2	15
Sensors (e. g., electromagnetic, electronic, acoustic)	12	3	15
Telephone taps and recorders	13	1	14
Pen registers	11	3	14
Telephone usage monitoring	7	3	10
Computer usage monitoring	4	2	6
Electronic mail monitoring or interception	1	5	6
Cellular radio interception	3	2	5
Pattern recognition systems	2	2	4
Satellite interception	1	3	4
Expert systems/artificial intelligence	0	3	3
Voice recognition	0	3	3
Satellite-based visual surveillance systems	1	1	2
Microwave interception	1	1	2
Fiber optic interception	0	1	1

SOURCE-Office of Technology Assessment

Table 5.—Agency Components Indicating the Largest Projected Use of Electronic Surveillance Technologies

Agency	Number of current plus planned technologies
Federal Bureau of Investigation (DOJ)	17
Office of the Inspector General (DOD),	13
Drug Enforcement Administration (DOJ)	11
U.S. Customs (Treasury)	10
U.S. Air Force (DOD)	9
National Park Service (DOI)	9
Internal Revenue Service (Treasury)	9
Office of the Inspector General (USDA)	9
Agricultural Stabilization and Conservation Service (USDA)	9

SOURCE Off Ice of Technology Assessment

the network owner. Some believe that even fiber optic circuits can be tapped (but with difficulty), although this technology is so new that reliable information is scarce. The major electronic countermeasures include radiation shielding of electronic equipment (to prevent eavesdropping of signals given off by such equipment), spread-spectrum transmission, and encryption. Many technical experts believe that encryption is the only sure way to "protect any form of electronic communications end-to-end. "[8 9]

Policy

The history of electronic surveillance policy significantly involves all three branches of Government: the judiciary, Congress, and the executive branch. Key activities and policy actions are highlighted below.

Judicial

The courts have had a significant role in interpreting the Constitution and various statutes as they apply to electronic surveillance.

Constitutional questions regarding the legitimacy of the use of electronic surveillance devices under specific circumstances most often turn on an interpretation of fourth amendment protections. The fourth amendment provides that:

> The right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The critical triggering phrase of the fourth amendment is "searches and seizures. " If there is no search or seizure, then official behavior is not covered by the fourth amend--ment, and it need not be reasonable, based on probable cause, or carried out pursuant to a warrant. Although there may be statutory protections that require certain conduct, an individual does not have fourth amendment protections unless there is a search and seizure. The secondary triggering phrase of the fourth amendment is "unreasonable." Even if official conduct is regarded as a search or seizure, there is no invasion of fourth amendment pro-

[8] Horgan, op. cit., pp. 30, 31, 33, 34, 38.

[9] For further discussion of technical vulnerabilities and related security measures, see the forthcoming OTA study on "New Communications Technology: Implications for Privacy and Security" expected to be published in winter 1986/87.

tections if the conduct is reasonable. Determination of reasonableness depends on the judicial balancing of the individual interest, generally regarded as a privacy interest, against the governmental interest, including law and order, national security, internal security, and the proper administration of the laws. Reasonableness generally entails a predicate of probable cause and, with many exceptions, the issuance of a warrant.

The meaning and scope of the fourth amendment have involved judicial construction of these key phrases. Definition of "searches" has come to be a crazy patchwork quilt, depending partly on whether the search involves a person's body or home, partly on how public the activity is, partly on the degree of invasion or intrusiveness involved in conducting the search, partly on the facts of the case under consideration, and partly on who is on the Court.[10]

Searches using some form of electronic monitoring at first posed difficult problems for the Court because the searches did not comport with traditional definitions of a search-they did not involve physical trespassing and were often conducted in a public place. Until 1967, electronic monitoring of conversations was not regarded as a search under the fourth amendment.[11] In the landmark case of Katz v. United States (1967), the Court ruled that wiretapping was a search under the fourth amendment. As is often the result of landmark cases, subsequent legal analysis and judicial construction have raised more questions than the case first resolved. This is especially true with respect to the two phrases most important for subsequent legal decisions–a "reasonable expectation of privacy" [12] and "the fourth amendment protects people, not places. "[13]

Following Katz, judicial determination of whether a "search or seizure' '-has occurred depends on whether or not the individual has a "reasonable expectation of privacy" in the area or activity under surveillance. In determining whether or not an individual has such an expectation, the Supreme Court has adopted as its test the two-part formulation from Justice Harlan's concurring opinion:

> . first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable. " [14]

The subjective part of the test focuses attention on the means the individual employs to protect his or her privacy, e.g., closing the door of a phone booth or closing curtains. Additionally, the assumption of risk that the individual appears to take is considered in determining the individual's actual expectation of privacy. Under assumption of risk, an individual is presumed to assume the risk that another party to a conversation or activity may consent to a search. This assumption of risk prevails even if the consenting party is an informer or undercover agent. "

The objective part of the test looks to what society regards as a reasonable expectation of privacy. Yet, it requires this without specifying an objective referent. Is "society" today's opinion polls, longstanding norms and traditions, a reasonable person, or the knowledge that people have in common? The result of the objective part of the test is that the Court has implicitly constructed a continuum of circumstances under which society would regard an individual as having a reasonable expectation

[10] For summary of Supreme Court rulings see: Anthony G. Amsterdam, "Perspectives on the Fourth Amendment, " 58 *Minnesota Law Review 349 (1974);* and Peter Goldberger, "Consent, Expectation of Privacy, and the Meaning of 'Searches' in the Fourth Amendment, " 75 *The Journal of Criminal Law and Criminology' 319 (1984).*

[11] *See* app. 2A for summary of relevant Supreme Court opinions.

[12] *Katz v. United States,* 389 U.S. 347, 360 (1967).

[13] Id. at 351.

[14] Id. at 361.

[15] See the "false friends cases' '– United *States v. White,* 401 U.S. 745 (1971), *Hoffa v. United States, 385* U.S. 293 (1966), and *Lopez v. United States, 373* U.S. **427 (1967).** In *White* the Court ruled that agents can be wired for sound and still be covered by the assumption of risk, reasoning that the risk did not increase materially simply because the informers were transmitting the conversation electronically. See also: Eric F. Saunders, "Electronic Eavesdropping and the Right to Privacy, " 52 *Boston University Law Review 831 (1973). Smith v. Maryland, 442* U.S. 735 (1979) and *United States v. Knotts, 103 S.* Ct. 1081 (1983) suggest that an individual forfeits his expectation of privacy by risking the possibility that his activities will be revealed to the police.

of privacy. The continuum ranges from public places ("open fields," "in plain view," "public highway"), in which there is no objective expectation of privacy except in unusual circumstances, to the inside of one's home with the windows and curtains shut and the door bolted, in which there is an objective expectation of privacy. The objective expectation of privacy along the continuum (shopping centers, motels, offices, automobiles, and yards) depends on judicial interpretation. Recently, the Court has modified the objective element, referring to it as a "legitimate' expectation of privacy."

The second important component of Katz is the holding that "the fourth amendment protects people, not places." The question of what protection the fourth amendment offers people remains unanswered, and defining the scope of such protection still necessitates reference to places. Moreover, the distinction between "people" and "places" has raised the question of whether the fourth amendment still protects property interests, or whether it now protects only more personal interests. The issue of the protection afforded people as distinct from that afforded places has become more significant with the growth of third-party recordkeepers, e.g., banks. The thrust of the Court opinion in Katz seemed to represent an expansion, not a replacement, of the existing fourth amendment protections:

> The amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all.[17]

[16] First used by Justice Powell in *Couch v United States*, 409 U.S. 322 (1973) in rejecting a fourth amendment objection to an IRS summons and later used by Powell in *United States v. Miller*, 425 U.S. 435 (1976). In *Rakas v. Illinois*, 439 [J. S. 128 (1978), Justice Rehnquist referred to expectations of privacy "which the law recognizes as 'legitimate,'" This modification gives the objective part of the test a positive law, rather than societal expectation, meaning. This has practical as well as theoretical importance in that the courts would not ask whether society would regard an expectation of privacy in a particular case as reasonable, but would instead examine the laws to determine expectation. Although this would require less subjective analysis by the courts, it seems to assume that the laws are correct and need not be evaluated against fundamental law, i, e., the fourth amendment. See Goldberger, op. cit., and Gerald G. Ashdown. "The Fourth Amendment and the 'Legitimate Expectation of Privacy,'" 34 *Vanderbilt law Review* 1289 (1981).

[17] *Katz v. United States*, 389 [J. S. 347, 350 (1967).

It has been argued that, based on Katz, analysis of privacy interests should replace the more traditional property analysis when the Government uses nonphysical methods of search and where relevant privacy interests do not have physical characteristics. The property aspect is viewed as still important because it gives specificity and concreteness to fourth amendment analysis.[18] Yet, in some recent rulings the Court has treated privacy as the only interest protected by the fourth amendment.[19] This implies a further narrowing of fourth amendment protection, both because property interests are not considered and because of the problems of defining privacy. As one legal commentator, concerned with the influx of new surveillance devices, noted:

> Confusion over the fourth amendment status of the beeper is unavoidable so long as privacy remains the central theoretical focus of fourth amendment analysis. Privacy, like most concepts of fundamental value, is a relative, indeterminate concept that is not *easily* converted into a workable legal standard.[20]

In evaluating the appropriateness of the use of electronic surveillance technologies by Government officials, the courts have worked within the framework established by *Katz*. *By analogy* to traditional surveillance devices, the courts have attempted to determine whether or not individuals have a "reasonable expectation of privacy." This becomes more difficult as surveillance devices become more technologically sophisticated because the analogy is often more remote and hence less convincing. The courts have generally continued to consider the place in which a surveillance device is located or the place that a device is monitoring. The courts generally have adopted the more expansive interpretation of Katz and have not abandoned higher levels of protection for certain places, e.g., homes and yards.

Yet, the Katz framework has not offered the courts sufficient policy guidance to deal with the range and uses of new surveillance tech-

[18] Note, "'Tracking *Katz*: Beepers, Privacy and the Fourth Amendment," 86 *Yale Law Journal*, pp 1461, 1479-80 (1977).

[19] Ashdown, op. cit., p. 1321.

[20] Note, *Yale Law Journal*, op. cit., p. 1477.

nologies. "Reasonable expectation of privacy" is an inherently nebulous phrase and, despite 20 years of judicial application, predicting its meaning in a new context is difficult. Determining whether a place is sufficiently private to offer protection against official surveillance is more and more difficult as the public sphere of activities encroaches on what was once deemed private.

Thus, the courts have, on several occasions, asked Congress to legislate in the area of electronic surveillance technology." Most *recently,* Judge Richard Posner, in a case involving the use of video surveillance, said:

> We would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III [of the 1968 Omnibus Crime Control and Safe Streets Act] to bring television surveillance within its scope. [22]

Congressional [23]

Congress did not play an active or effective role in surveillance policy until 1968. Prior to that time, the only legislation affecting official use of surveillance technology was unintended. In 1934, Congress remodified the Radio Act of 1927 as the Communications Act. Section 605 of the 1934 Act provided that "No person not being authorized by the sender shall intercept any communication and divulge . . . the contents. " There was no specific legislative history for this section and it appears that the 1934 bill was not intended to change existing law.[24] This was the interpretation until 1938 when the Supreme Court, in *Nardone v. United States,* 302 U.S. 379, ruled that Section 605 prohibited all telephone wiretapping, even when done by Federal Government officers. In response, bills passed both houses of Congress allowing wiretapping under certain circumstances and with certain procedural requirements. But the session ended before the conference committee could resolve a difference between the two bills-the House bill explicitly criminalized unauthorized official surveillance.[25]

Despite Congress's failure to overrule Nar*done* by legislation, wiretapping continued because the Justice Department construed Section 605 as not prohibiting wiretapping itself, but only the interception and subsequent divulgence outside the Federal establishment. Additionally, the President issued an Executive order to allow wiretapping for national security purposes.

In the immediate post-war period, numerous bills authorizing electronic surveillance were introduced, but none was enacted into law. Starting in 1960, electronic surveillance became a major public issue and congressional activity became more focused and purposeful. The target was organized crime, a major priority of the Kennedy Administration.

The first major congressional action regarding surveillance was Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Because it has served as a model for controlling Government surveillance, analysis of the statute is necessary.

The basic legislative history document, S. Rep. No. 1097, 90th Cong., 3d sess. (1968), describes the purpose of the statute as follows:

> ITlhe U.S. Supreme Court, on June 12,1967, handed down the decision in *Berger v. New York,* 388 U.S. 41, which declared unconstitutional the New York State statute authorizing electronic eavesdropping (bugging) by law enforcement officers in investigating certain types of crimes. The Court held that the New York statute, on its face, failed to meet certain constitutional standards. In the course of the opinion, the Court delineated the constitutional criteria that electronic surveillance legislation should contain. Title III was drafted to meet these standards and to conform with *Katz v. United States,* 389 U.S. 347 (1967).

---

[21] See, for example, *United States v. U.S. District Court (Keith), 407* U.S. 297 (1972) in which the court suggested that Congress should devise a scheme for foreign intelligence.

[22] *United States v. Torres,* No. 84-1077, p. 19 (7th Cir., Dec. 19, 1984).

[23] Material in this section is derived in large part from Herman Schwartz, "Surveillance: Historical Policy Review, " OTA contractor paper, March 1985.

[24] See: S. Rep. No. 781, 73 Cong., 2d sess. 11 (1934).

[25] See: S. Rep. No. 1790, 75th Cong., 3d sess. 3 (1983).

> Title 111 has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. "

The problem the statute was designed to solve was seen as a combination of "tremendous scientific and technological developments that have taken place in the last century [that] have made possible today the widespread use and abuse of electronic surveillance techniques, and "a body of law [that] from the point of view of privacy or justice [i.e., law enforcement] is . . . totally unsatisfactory. "[27] The preamble to Title III reflects these aims: 1) to obtain evidence of "certain major types of offenses, and to cope with "organized criminals and 2) to safeguard the privacy of innocent persons and to provide "assurances that the interception is justified and that the information obtained thereby will not be misused.

In order to achieve these purposes, the statute provides that electronic surveillance of conversations is prohibited, upon pain of a substantial jail sentence and fine, except for: 1) law enforcement surveillance under a court order; 2) certain telephone company monitoring to ensure adequate services or to protect company property; 3) surveillance of a conversation where one participant consents to the surveillance; and 4) surveillance covered by the Foreign Intelligence Surveillance Act of 1978 (as Title 111 was later amended). I.aw enforcement surveillance must meet certain procedural requirements, which include:

1. an application for a court order approved by a high-ranking prosecutor (not by a policeman);
2. surveillance only for one of the crimes specified in Title III (the list was expanded in the early 1970s and again in October 1984 in the Comprehensive Crime Control Act);
3. probable cause to believe that a crime has occurred, the target of the surveillance is involved, and the evidence of that crime will be obtained by the surveillance;
4. a statement indicating that other investigative procedures are ineffective; and
5. an effort to minimize the interception.

A judge must pass on the application and may issue the order, and any extensions, if it meets the statutory requirements. Shortly after the surveillance ends, notice of the surveillance must be given to some or all of the people affected, as the judge decides, unless the judge agrees to postpone the notice. Illegally obtained evidence may not be used in any official proceedings, and a suit for damages may be brought for illegal surveillance, though a very strong good faith defense is allowed. In addition, the manufacture, distribution, possession, and advertising of devices for electronic surveillance for nonpublic use are prohibited.

There was little discussion of electronic surveillance by State officials during the legislative debates. Nevertheless, $2516(2) of Title III gives State officials wiretapping authority, if a State passes legislation modeled on the Federal act, for the investigation of:

> . . . murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marijuana or other dangerous drugs, or other crime dangerous to life, limb or property and punishable by imprisonment for more than one year . . . or any conspiracy to commit any of the foregoing offenses.

As of December 31, 1984, some 29 States and the District of Columbia have authorized their law enforcement officials to wiretap, though the State statutes differ in various ways.

On its face, Title III covers the interception of only conversations that are capable of be-

---

[26] Id. at 66. Three definitions in Title 11 I are important in determining the scope of the act:

1 *wire communication* means any communication made in w hole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign commu nications,

2 *oral communication* me an> any oral communication uttered by a person exhibiting an expectation that such communication is not subject to Interception under circumstances justifying such expectation: and

3 *intercept* means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device (Section 251() of Title 111)

[27] Id. at 67, 69.

ing heard by the human ear; data transmission, the video part of videotaping, pen registers, and other forms of communication are not covered. [28] The statute also permits interception for official purposes where one of the parties to the conversation has consented to the interception; private interceptions where one party consents are also exempt from the statutory ban unless the interception is for a criminal, "injurious," or tortious purpose. Evidence obtained in violation of the statute is excluded from all judicial or administrative proceedings, but only someone whose privacy was invaded can challenge the evidence.

The other major statute regulating the use of surveillance devices by Government officials is the Foreign Intelligence Surveillance Act of 1978 (FISA). This act establishes legal standards and procedures for the use of electronic surveillance in collecting foreign intelligence and counter-intelligence within the United States. This was the first legislative authorization for foreign intelligence wiretapping and other forms of electronic surveillance.'[8] The scope of this act is broader than Title III. FISA defines electronic surveillance broadly to include four categories: 1) *wiretaps,* including not only voice communications but also teleprinter, telegraph, facsimile, and digital communications; 2) *radio intercepts; 3) monitoring devices,* which may include microphone eavesdropping, surreptitious closed circuit television (CCTV) monitoring, transmitters that track movements of vehicles, and other techniques; and 4) *watch listing.* However, the application of FISA protection in the latter three categories is limited to those circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. [30] The act created the Foreign Intelligence Surveillance Court, composed of seven Federal District Judges, to review and approve surveillance capable of monitoring U.S. persons (defined as U.S. citizens, lawfully admitted permanent resident aliens, and domestic organizations or corporations that are not openly acknowledged to be directed and controlled by foreign governments) in the United States. The procedural requirements of FISA apply only to electronic surveillance for foreign intelligence purposes, but the criminal penalties appear to apply more broadly to include law enforcement surveillance.[31]

There are a number of other statutes that place controls on the procedures and techniques of Government surveillance depending on the type of information that is being sought, e.g., the Privacy Act of 1974, the Right to Financial Privacy Act of 1978, the Electronic Funds Transfer Act of 1980, the Privacy Protection Act of 1980, and the Cable Communications Policy Act of 1984. (See appendix 2B for a summary of these statutes.)

Executive

Because of ambiguities in existing laws, executive officials have issued orders and guidelines to clarify the application of specific statutes or protections under particular circumstances or with respect to certain technological devices. Clarification of the scope and intent of FISA can be found in a number of Executive orders.[32]

In the absence of statutory or judicial guidance in the use of electronic surveillance for law enforcement and intelligence purposes, the Department of Justice (DOJ) generally issues policy guidelines that are regarded as requirements on agents of DOJ bureaus (FBI, Immigration and Naturalization Service, and Drug Enforcement Administration), and are usually considered as advisory by other agencies engaged in surveillance activities (e.g., Customs, Bureau of Alcohol, Tobacco and Firearms, IRS). For example, DOJ has issued policy guidelines for the use of electronic

[28] See S. Rep. No. 1097 at 90 (pen registers, etc., not included).
[29] See S. Rep. No, 98-660, "The Foreign Intelligence Surveillance Act of 1978: The First Five Years, " p. 1.
[30] Id. at 4.
[31] See Mar. 9, 1984 letter from John Keeney of the U.S. Department of Justice to U.S. Senator Patrick Leahy.
[32] See, e.g., Executive Order No. 12036, "United States Intelligence Activities, " Jan. 24, 1978 and updated as Executive Order No. 12333 on Dec. 4, 1981; also Executive Order No. 12139, "Exercise of Certain Authority Regarding Electronic Surveillance, " May 23, 1979.

visual surveillance and the use of pen registers. Such guidelines are issued to ensure that there are adequate procedural and substantive protections for individuals who are subject to surveillance, and that, therefore, information that is gathered through such surveillance will not be excluded as evidence in court,

FINDINGS AND POLICY IMPLICATIONS

1. The existing statutory framework and judicial interpretations thereof do not adequately cover new electronic surveillance technologies. Indeed, some courts have asked Congress for guidance on the new technologies,

See preceding discussion of policy history and background.

2. Despite a lack of coordination in electronic surveillance policymaking among the three branches of Government and the ad hoc nature of that policy, there are seven general components that are found in existing policies, be they legislative, executive, or judicial. Although the specifics of these components will vary given the different types of electronic surveillance being used, the general model is the same.

The first component of surveillance policies is a way of checking on the discretion of the Government agent in the field over whether to institute such surveillance. This can range from a field supervisor's approval to department-level approval to a U.S. Attorney's approval to a judicial warrant. The critical distinction in terms of level of approval necessary is whether the executive branch agency is responsible for authorizing the electronic surveillance or whether judicial approval is also necessary. In terms of checking agent discretion, judicial approval obviously represents a higher standard.

The second component is a listing of the crimes or circumstances for which a particular type of electronic surveillance is considered appropriate. Title 111 is a good example of this, as is the Foreign Intelligence Surveillance Act. In some situations, the list maybe quite broad but the principle remains. Crimes are categorized as misdemeanors and felonies with classes within each group. Electronic surveillance is generally only used for investigations of major felonies. Circumstances are often defined in terms of the governmental interest in pursuing the investigation. There is an implicit ranking of the importance of governmental interests for which surveillance devices are employed—national security, domestic security, law enforcement, and the proper administration of Government programs.

The third component of surveillance policies is some standard to indicate the degree of confidence about alleged criminal behavior that is necessary before the use of a particular surveillance technique is appropriate. This involves a showing of the evidence that has been accumulated to date, and a showing that the target of surveillance will provide additional evidence. The standard may range from probable cause, to reasonable suspicion, to reason to believe, to no need for any showing of evidence.

The fourth component is some justification for the need to use a particular surveillance technique or device. Generally, this requires a showing that more traditional forms of surveillance have failed, and some explanation as to how the surveillance technique under discussion will secure the necessary information.

The fifth component of surveillance policies is a requirement for an account of how the scope of the surveillance will be minimized to the particular party or parties under investigation and to those activities that seem criminally related.

The sixth component is the requirement that the individual be given some notice after the fact that he or she has been subject to surveillance, except in circumstances where notice would jeopardize an investigation or national security interests. There is no provision for notice in FISA, unless the party is being prosecuted.

The seventh component is a statement of the sanctions that apply if evidence is not collected in conformity with the requirements of the statute. An example of this is the exclusionary rule. Additionally, some statutes contain penalties for investigative agents who violate the statute, thus providing the individual with a civil remedy.

3. In applying the major components of electronic surveillance policy, the legislature, executive agency, or court, implicitly or explicitly, uses a framework for analysis. This framework involves balancing the societal interest in maintaining civil liberties protections for the individual against the societal interest in successful Government investigations. Based on an evaluation of previous policy formulation, it appears that policy makers, more or less consciously, have looked at certain dimensions in determining this balance.

Table 6 outlines the dimensions of the civil liberty interest v. the Government investigative interest found in existing electronic surveillance policy.

The dimensions of a civil liberty interest provide, to some extent, indicators for a "reasonable expectation of privacy" (Katz test) and the level of intrusiveness of the surveillance technology. In general, the more intrusive the technology, the more it violates "expectations of privacy' and the greater the threat to civil liberties. This has been an accepted principle since surveillance technologies were first used. Prior to Katz, the fourth amendment was interpreted to mean that "unreasonable" searches required physical intrusion into a constitutionally protected area. Following *Katz,* the physical trespass requirement was dropped. The Court has implicitly, if not often explicitly, continued to consider the intrusiveness of a search in determining its reasonableness, but intrusion is more broadly construed to go beyond mere physical trespass.

The difficulty in using intrusiveness as a principle by which to evaluate an "expectation of privacy" and the appropriateness of using a particular surveillance device is that no criteria have yet been explicitly formulated to determine intrusiveness. Instead, the facts of individual cases seem to be determinative. Yet, based on court rulings, congressional statutes, and executive orders, it is possible to isolate five dimensions that are important in determining the level of intrusiveness and the civil liberties interest that warrants protection.

Table 6.—Dimensions for Balancing Civil Liberty Interest v. Government Investigative Interest

Civil liberty *interest:*

1. *Nature of information:* The more personal or intimate the information that is to be gathered about a target, the more intrusive the surveillance technique and the greater the threat to civil liberties.
2. *Nature of p/ace communication.'* The more "private" the area or type of communication to be placed under surveillance, the more intrusive the surveillance and the greater the threat to civil liberties
3. *Scope of surveillance:* The more people and activities that are subject to surveillance, the more intrusive the surveillance and the greater the threat to civil liberties.
4. Surreptitiousness *of surveillance.'* The less likely it is for the individual to be aware of the surveillance and the harder it is for the individual to detect it, the greater the threat to civil liberties.
5. *Pre-electronlc analogy:* Pre-electronic analogies are often considered in determining ıntrusivenes[s], but with widely varying interpretations.

Government investigative intersert:

1 *Purpose of investigation:* Importance ranked as follows: national security, domestic security, law enforcement, and the proper administration of Government programs,
2. *Degree of individualized suspicion.* The lower the level of suspicion, the harder it is to justify the use of surveillance devices.
3, *Relative effectiveness:* More traditional Investigative techniques should be used and proven ineffective before using technologically sophisticated techniques.

SOURCE Off Ice of Technology Assessment

The first dimension is the nature of the information (content) that can be acquired. The more personal or intimate the information that is gathered, the more intrusive the surveillance technique and the greater the threat to civil liberties. Although ambiguous or incomplete information poses a threat to civil liberties, a surveillance technique that gathers more detailed information is generally regarded as more intrusive than one that gathers less detailed information. As a way of evaluating the specificity of information, the categorization of types of behavior that may be subject to surveillance (and illustrative surveillance technologies) may be useful (see table 2). Under this scheme, a surveillance technique that gathers information on movements would be

regarded as less intrusive than one that gathers information on actions and communication.

The second dimension is the "public" or "private" nature of the area (place) or communication to be placed under surveillance. The fourth amendment explicitly protects persons, houses, papers, and effects. The difficulty is that these can be more private or less private depending on where they are kept or who else is given access to them, Homes, phone conversations, and first class mail have traditionally been regarded as "private." In general, the more "private" the area or communication, the more intrusive the surveillance and the greater the threat to civil liberties.

The third dimension is the scope of the surveillance or the extent to which the surveillance covers persons not specifically under surveillance.[33] The importance of this principle is reflected in the minimization requirements of Title III and FISA. The broader the net cast, the more intrusive the surveillance and the greater the threat to civil liberties.

The fourth dimension is the surreptitiousness of the surveillance or the individual's ability to detect whether he or she is the target of surveillance. This ability to detect involves both the likelihood that the individual will be aware of the surveillance and also his or her ability to locate the source. This dimension is reflected in the concept of assumption of risk, which has been used as a justification for one-party consent to surveillance. It is also reflected in the lower standards for physical surveillance because it is assumed that an individual can easily monitor whether or not someone is following him or her. The harder it is for the individual' to detect the surveillance, the greater the threat to civil liberties.

The final factor that policymakers often consider in evaluating the civil liberty threat of an electronic surveillance device is the pre-electronic analogy of the surveillance technique. This focuses attention on a historical measure of privacy that provides a standard for preserving a certain level of privacy. Analogies are made to policy choices for a pre-electronic era. For example, what kinds of communications have traditionally been protected, i.e., first class mail and phone calls, and what modern communications are their counterparts? Two policy difficulties are presented by this factor. The first is that different people see different analogies. The second is that the intrusiveness of a pre-electronic device and its electronic counterpart is not always correspondent.

In evaluating the legitimacy of the Government's use of surveillance devices, three dimensions are considered. The first is the purpose of the investigation (the governmental interest). There is an implicit ranking of the importance of governmental interests for which investigations are carried out—national security, domestic security, law enforcement, and the proper administration of Government programs. The nature of the governmental interest determines the level of judicial or administrative control, both initially and at specified review stages. With respect to the use of electronic surveillance, the importance of the governmental interest is always considered, but is not determinative of the level of surveillance. The law enforcement interest is broadest, but most well developed in statute, e.g., Title III categories of crimes for which eavesdropping may be used. The national security and domestic security purposes have constitutionally allowed Government officials the greatest discretion in determining whether surveillance should be used. The rules for administrative searches are fairly well developed in statutes, but standards for the use of electronic surveillance often are not included.

The second dimension is the degree of individualized suspicion. In general, the earlier in the investigation the harder it is to justify the use of surveillance devices. This is so because it may be difficult to document that criminality is involved and that the target of

[33] See Donald L. Doerenberg, " 'The Right of the People': Reconciling Collective and Individual Interests Under the Fourth Amendment, " 58 *New York University Law Review 259 (1983),* who distinguishes the following possible targets of a search—all citizens, categories or classes of individuals, or a selected individual.

the surveillance is involved or can provide evidence. Traditionally, the standard for the Government's need to know varies depending on what it already knows. In theory, the more the Government knows, the less likely that it is engaging in a fishing expedition. If the Government has probable cause to believe that someone is implicated in a crime or terrorist activity, then it has a need to know more than if it had only a reasonable suspicion or reason to believe that someone was involved.

The third dimension is the relative effectiveness of electronic surveillance compared to other means that are available to secure the same information. In existing policies, the assumption is that there should be a demonstration that more traditional investigative techniques have been used and proven ineffective before using technologically sophisticated electronic techniques. An analysis of the effectiveness of the surveillance technology or device is important in determining the legitimacy of its use. If more accurate and complete evidence can be gathered through the use of an electronic surveillance device than through pre-electronic means, then serious consideration will be given to its use.

The following chapters describe a number of new electronic surveillance devices and techniques that have been made possible by technological advances and analyze their policy implications using the framework developed in this chapter.

APPENDIX 2A: KEY SUPREME COURT DECISIONS ON ELECTRONIC SURVEILLANCE

Olmstead v. United States, 277 U.S. 438 (1928)—a 5-4 decision ruling that neither the fourth nor fifth amendments to the Constitution applied to wiretapping. The fourth amendment did not apply because: there was no trespass; its protection is limited to material effects, not to intangibles like speech; and there was no protection for voice communication projected outside the house. The fifth amendment did not apply because there was no evidence of compulsion to talk over the phone and because the fourth was not first violated. Brandeis argued in his dissent that the fourth amendment protected a right to privacy, and stated:

> Moreover, "in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related science may bring means of exploring unexpressed beliefs, thoughts and emotions. . . Can it be that the Constitution affords no protection against such invasions of individual security?

Public reaction to the decision was negative; bills were introduced in Congress, but none passed.

Nardone v. United States, 302 U.S. 379 (1937)–Court ruled that Section 605 prohibited telephone wiretapping by anyone, including Federal Government officers. Decision was criticized as "judicial legislation." Bills were introduced in Congress to allow wiretapping under certain circumstances, but none passed. Evidence indicates that wiretapping continued at the time despite decision.

Berger v. New York, 388 U.S. 41 (1967)–Court declared the New York wiretapping statute unconstitutional because it was not particular enough in describing the crime, or "the place to be searched," or the "persons or things to be seized" as specifically required by the fourth amendment.

Katz v. United States, 389 U.S. 347 (1967)–Court overruled *Olmstead,* thus bringing wiretapping under the fourth amendment. The Court developed a general formula to determine whether an investigative technique conflicts with the fourth amendment–does the individual evidence an expectation of privacy and is the expectation of privacy "one that society is prepared to recognize as 'reasonable?' " The Court's criteria for valid surveillance involved a warrant, particularization and probable cause requirements for suspect, crime, phone, and time.

United States v. U.S. District Court for the Eastern District of Michigan, 407 U.S. 297 (1972)–Court prohibited unauthorized electronic surveil-

lance to gather intelligence for domestic security purposes, holding that:

> . . . prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.

United States v. Miller, 425 U.S. 435 (1976)–Court ruled that a bank customer's financial record is the property of the bank, and thus he or she has no legitimate "expectation of privacy" in these records.

United States v. New York Telephone Co., 434 U.S. 159 (1977)–Court held that to be covered by Title III, a communication must be capable of being overheard.

Smith v. Maryland, 442 U.S. 735 (1979)–Court held that the use of a pen register did not violate the fourth amendment.

United States v. Knotts, 103 S. Ct. 1081 (1983) –Court held that the *warrantless* monitoring of a beeper is not a search and seizure under the fourth amendment because there is no reasonable expectation of privacy as the movements tracked are public.

United States v. Karo, 104 S. Ct. 3296 (1984)–Court held that using a beeper to trail a container into a house and "to keep in touch with it inside the house" did violate the fourth amendment.

APPENDIX 2B: KEY STATUTES RELEVANT TO ELECTRONIC SURVEILLANCE

Section 605 *of the Communications Act of 1934* provided that "No person not being authorized by the sender shall intercept any communication and divulge . . . the contents . . ."

Title III of the 1968 Omnibus Crime Control and Safe Streets Act is designed to protect the privacy of wire and oral communications and also to allow evidence to be obtained for "certain types of major offenses. " Law enforcement electronic surveillance of conversations is thus prohibited except under a court order, which a judge may issue after being convinced that the following procedural requirements have been met:

1. application by a high-ranking prosecutor;
2. surveillance for one of the crimes specified in Title III;
3. probable cause to believe that a crime has occurred, that the target of the surveillance is involved, and that the evidence of that crime will be obtained by the surveillance;
4. a statement indicating that other investigative procedures are ineffective; and
5. an effort to minimize the interception.

Crime Control Act of 1973 requires-that State criminal justice information systems, developed with Federal funds, be protected by measures to ensure the privacy and security of information.

Privacy Act of 1974 requires agencies to comply with fair information practices in their handling of personal information, including the following: records must be necessary, lawful, current, and accurate; records must be used only for purpose collected except with an individual's consent or where exempted; no record of an individual's exercise of first amendment rights is to be kept unless authorized by statute; information cannot be sold or rented for mailing list use. The following are exempted: CIA records; records maintained by law enforcement agencies; Secret Service records; Federal testing materials; etc.

*Foreign Intelligence Surveillance Act of 1978 es*tablishes legal standards and procedures for the use of electronic surveillance to collect foreign intelligence and counter-intelligence within the United States. This was the first legislative authorization for wiretapping and other forms of electronic surveillance (including radio intercepts, microphone eavesdropping, closed circuit television, beepers, and other monitoring techniques). It created the Foreign Intelligence Surveillance Court, composed of seven Federal District Judges, to review and approve surveillance capable of monitoring U.S. persons (defined as U.S. citizens, lawfully admitted permanent resident aliens, and domestic organizations or corporations that are not openly acknowledged to be directed and controlled by foreign governments) in the United States. The procedural requirements of FISA apply only to electronic surveillance for foreign intelligence purposes, but the criminal penalties appear to apply more broadly to include law enforcement surveillance.

Right to Financial Privacy Act of 1978 provides bank customers with some privacy regarding their

records held by banks and other financial institutions, and provides procedures whereby Federal agencies can gain access to such records.

Electronic Funds Transfer Act of 1980 provides that any institution providing EFT or other bank services must notify its customers about third-party access to customer accounts.

Privacy Protection Act of 1980 prohibits Government agents from conducting unannounced searches of press offices and files if no one in the press room is suspected of a crime.

Cable Communications Policy Act of 1984 requires the cable service to inform the subscriber of: the nature of personally identifiable information collected and the nature of the use of such information; the disclosures that may be made of such information; the period during which such information will be maintained; and the times during which an individual may access such information. Also places restrictions on the cable services' collection and disclosures of such information. The act creates a subscriber right to privacy against Government surveillance.

Chapter 3

Telephone Surveillance

Chapter 3
Telephone Surveillance

SUMMARY

The public generally expects that telephone conversations are private, and that electronic surveillance of telephone calls (sometimes known as wiretapping or eavesdropping) is illegal, except in very narrowly circumscribed law enforcement and national security investigations. But technological innovations now make it easier to electronically monitor both the content of phone calls and phone transactions (e.g., number called, time, and place called). Furthermore, the new telephone technology was not envisioned when current legal protections were enacted, and thus the statutory protection against telephone surveillance is weak, ambiguous, or nonexistent.

After reviewing and assessing relevant technological developments and the statutory framework, OTA found that:

- A host of new information technologies has revolutionized the telephone system since 1968—the last time Congress passed major legislation (Title III of the Omnibus Crime Control and Safe Streets Act) that covered telephone surveillance by law enforcement agencies and private parties.
- Significant new technologies include digital transmission (whereby many phone calls are converted from analog to digital form for transmission) and cellular and cordless phones, as well as the increased use of telephones for electronic transmission of data.
- Deregulation of the telephone industry, the proliferation of common carriers, and the growth of private (as opposed to common carrier) telephone companies also raise questions as to the applicability of existing legal protections for telephone privacy.
- The contents of phone conversations that are transmitted in digital form or made on cellular or cordless phones are *not* clearly protected by existing statutory and constitutional prohibitions on the interception of phone calls.
- Interception of the content of phone calls represents a substantial threat to civil liberties, but also a significant benefit to investigative authorities. This balancing is reflected in the standards and procedures presently embodied in Title III for such interception.
- New information technologies–e.g., advanced pen registers and automatic billing equipment—have also greatly increased the ability to collect and access transactional information about telephone calls (e.g., the numbers and places called).
- Transactional information is also *not* clearly protected under existing statutes and judicial precedents.

OTA identified three major options for congressional consideration with respect to policy on interception of the content of telephone calls:

- treat all calls similarly with respect to the extent of protection against unauthorized interception, i.e., extend Title III of the Omnibus Crime Control and Safe Streets Act to cover all phone calls-whether analog, digital, cellular, or cordless-and both voice and data communications;
- formulate special policies for specific telephone technologies; and
- do nothing and leave policymaking up to the development of case law depending on individual circumstances.

OTA also concluded that the deregulatory and market trends toward private telephone systems and hybrid common carrier-private systems indicate the need for congressional review of applicable provisions of the Commu-

nications Act of 1934 and Federal Communications Commission regulations, as well as Title III of the Omnibus Crime Control Act, with respect to telephone privacy protection.

Finally, OTA concluded that at present there is no feasible and cost-effective technological method to provide universal protection against telephone surveillance. A separate OTA study is examining future technical trends and safeguards against misuse as well as issues and options relevant to monitoring of transactional-as contrasted with content—information. *

*See the separate OTA study on "New Communications Technology: Implications for Privacy and Security," expected to be published in winter 1986/87.

INTRODUCTION

Most phone users have assumed a high degree of confidentiality for their phone calls. This has been especially true as private lines and improved connections replaced party lines and broken connections. In some respects, the technology has brought more assurances for the protection of the privacy of phone calls than did the law. However, this is now changing. Four technological innovations in phone service—digital transmission, new types of phones, new phone networks, and the ability to easily collect detailed information on phone usage—make it easier both to overhear the content of phone calls and also to monitor phone transactions. The law has not yet addressed these innovations, thus leaving gaps between the privacy that people expect and the privacy that they are assured.

With the conventional telephone, phone calls were transmitted in analog form across wire lines. Today, an increasing percentage of phone calls are converted from analog to digital form and then transmitted. Transmission may be over wire, but is often via microwave radio and satellite systems and, increasingly, via fiber optic transmission facilities. Statutes prohibiting wiretapping, primarily Title III of the Omnibus Crime Control and Safe Streets Act, were written to regulate the interception of oral communications transmitted in whole or in part by wire.

Additionally, new phones are making use, in whole or in part, of radio communications. Cellular or mobile phones use radio to transmit messages between a phone and a switching center, while cordless phones use radio to carry messages between the phone base station and the cordless phone handset. Section 605 of the 1934 Communications Act prohibits interception of radio communications. However, it does not protect phone calls because the courts have ruled that Congress intended Title III to be the exclusive remedy with respect to telephone interceptions.

Another growing gap in the protection afforded phone calls is between common carrier calls and private network calls. Legislation has addressed the former, while the latter have not been given any legal protection. Thus, the privacy of the content of digitized phone calls, cellular and cordless phone calls, and private carrier calls may not be afforded protection against interception by either Government officials or private parties.

Moreover, technological changes make it far easier today to monitor phone transactions. Pen registers are devices by which Government officials or private parties can monitor the numbers dialed on a given line. Presently, a court order is not necessary to install a pen register under Title III or the fourth amendment, but is required under the Foreign Intelligence Surveillance Act. Increasingly, computerized telecommunications switching equipment can collect and store information on the numbers dialed and length of phone calls. This information may be kept for billing and administrative purposes, but it also has monitoring capabilities. As automatic call accounting becomes widespread, pen registers will become unnecessary. A detailed historical record of long-distance and sometimes lo-

cal phone calls is now kept for perhaps 3 months by phone companies and can be accessed by Government officials with a subpoena. However, if a phone system is wholly or in part private, then this calling information is legally available to Government officials without a subpoena.

Before analyzing in detail the policy issues presented by these gaps in the protection for the content of phone calls and the record of phone transactions, a brief review of the history and background of technology and policy regarding wiretapping will be presented.

BACKGROUND[1]

Telegraph and telephone tapping by both private citizens and public officials began soon after the telegraph and telephone were invented. Some States tried to deal with telephone tapping either through their trespass statutes or by expanding early laws barring telegraph interceptions. However, the legality of Government surveillance under these statutes was usually unclear because there was no rule excluding illegally obtained evidence. By 1927, despite questions about the scope of coverage, some 28 States had made wiretapping a crime.[2]

Federal concern about wiretapping first surfaced in 1918 when the Federal Government began regulating the telephone system, but the concern was primarily for "the protection of the government and the property of the telephone and telegraph companies while under governmental control."[3] The Government barred tapping of, or interference with, telephone and telegraph messages, if the tap was done "without authority." This legislation expired in 1919. Civil liberties concerns first became important in the early 1920s, when wiretapping was used by the Department of Justice in its raids against aliens.[4] At this time, there were also reports that the phones and offices of members of Congress had been eavesdropped on.

In 1924, Attorney General Harlan Fiske Stone banned wiretapping by the Department of Justice, including the Bureau of Investigation (the FBI's predecessor). This effort at administrative control was only partially successful. The order bound only the Department of Justice and not the Treasury, which had jurisdiction over Prohibition enforcement, the law enforcement area that came to rely most on electronic surveillance. Prohibition agents continued to wiretap, even though the Treasury Department purported to be officially opposed to wiretapping.[5]

The Treasury's wiretapping ultimately brought the matter to the courts in *Olmstead v. United States, 277* U.S. 438 (1928). The Court, in a *5-4* opinion by Chief Justice Taft, ruled that neither the fourth nor fifth amendments to the Constitution provided protection against wiretapping.[6] The public reaction to the *Olmstead* decision was largely and strongly negative.[7] Immediately after *Olmstead* was decided, bills were proposed in Congress to ban wiretapping.[8]

[1] Material in this section is based in part on Herman Schwartz, "Surveillance: Historical Policy Review," contractor paper prepared for OTA, March 1985.

[2] See *amicus* brief for the telephone companies in *Olmstead v. United States,* **277** U.S. 438 (1928).

[3] H. R. Rep. No. 800, 65th Cong., 2d sess. (1918), reprinted in *Wiretapping, Eavesdropping and the Bill of Rights,* Hearings Before the Subcommittee on Constitutional Rights of the Senate Judiciary Committee, Part 4, Appendix to Part 3, 86th Cong., 1st sess. 792 (1959) ("1914-1959 Leg. Hist.").

[4] Alan Westin, *The Wire-tapping Problem,* 52 *Columbia Law Review 164, 172* n. 35 (1952).

[5] Walter F. Murphy, *Wiretapping on Trial: A Case Study in the Judicial Process (New* York: Random House, 1965), p. 13.

[6] The Court gave three reasons why the fourth amendment was not implicated: 1) officials had not trespassed onto *Olmstead* property; 2) the amendment did not apply to intangibles like speech, but only to material "effects"; and 3) there was no protection for voice communications projected outside the house, Justice Holmes wrote a short dissent, condemning the agents' conduct as "dirty business." Justice Brandeis wrote the main dissent in which he disagreed with the majority's reading of the precedents, its very narrow view of the fourth amendment, and its willingness to countenance criminal activity by the Government. **1914-59** Leg. Hist. **770-73.**

[7] Murphy, op. cit., p. 125.

[8] 1914-59 Leg. Hist. 881-83.

In 1934, Congress remodified the Radio Act of 1927, which was itself a recodification of legislation going back to 1912. Section 605 of the 1934 Act provided that:

> No person not being authorized by the sender shall intercept any communication and divulge . . . the contents . . .

There was no specific legislative history for this section and it appears that the 1934 bill was not intended to change existing law.[9] Apparently no one thought Congress had taken an important step in dealing with electronic surveillance.

It thus came as a surprise to many when the Supreme Court in 1938 ruled that Section 605 prohibited all telephone wiretapping, even when done by Federal Government officers.[10] In 1957, the Court ruled that this applied to State officers as well.[11] The Nardone decision was generally criticized both in 1938 and later as "judicial legislation. "[12]

Congressional response to Nardone was swift, but did not result in legislation. This time, bills were introduced to allow wiretapping, provided that the head of a department believed a felony had been or was about to be committed by two or more people. Congressional concern about organized crime was one of the two primary reasons for authorizing electronic surveillance, the other being national security. Bills allowing wiretapping passed both houses, but the session ended before the conference committee could resolve a difference between the two bills-the House bill explicitly criminalized unauthorized official surveillance.[13] The ease with which both Houses passed bills allowing Federal surveillance might lead one to think legislation was imminent. But this did not happen, even though, despite the *Nardone* decision, the Federal Government and State officials continued to wiretap.[14]

During and after World War II, the FBI engaged in large amounts of electronic surveillance. Between 1940 and 1960, the FBI installed over 7,000 national security surveillances, with 519 taps and 186 bugs in 1945 alone; and the Treasury Department installed over 10,000 taps during 1934 to 1948. Other Federal agencies, like the military, also engaged in tapping and bugging. On the local level, the New York City police installed thousands of taps each year (e.g., 3,588 in 1953-54), mostly in morals and bookmaking investigations; studies by Samuel Dash and others have documented widespread tapping elsewhere.[15]

The tapping and bugging targeted many people who might not normally appear to be appropriate targets, a situation that continued at least into the 1960s. In 1941, for example, the Los Angeles Chamber of Commerce was tapped, on the authority of Attorney General Francis Biddle. Presidential aides and others were similarly tapped. The most complete information on these practices, as developed by the Church Committee, relates to FBI surveillances in the post-1960 period when Dr. Martin Luther King, Jr., Congressman Harold Cooley, journalists, and many others were put under electronic surveillance. [16]

At this time, questions were also being raised concerning the effectiveness of electronic surveillance and of judicial protections, as well as the persistent use of electronic surveillance in State law enforcement for minor crimes. [17] There was also much documentation

---

[9] See S. Rep. No. 781, 73d Cong., 2d sess. 11 (1934), reprinted in 1914-59 Leg. History 895; Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance 35 (1976).

[10] *Nardone v. United States,* 302 U.S. 379 (1937).

[11] *Benanti v. United States,* 355 U.S. 96 (1957).

[12] Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, *Electronic Surveillance* (Washington, DC: NWC, 1976), p. 35.

[13] S. Rep. No. 1790, 75th Cong., 3d sess. 3 (1938), reprinted in 1914-59 Leg. Hist. 961; Murphy, op. cit., p. 135.

[14] See generally Samuel Dash, Richard F. Schwartz, and Robert E. Knowlton, *The Eavesdroppers (New* York: DeCapo, 1959).

[15] Ibid.; and Herman Schwartz, *Taps, Bugs, and Fooling the People (New* York: Field Foundation, 1977).

[16] See U.S. Congress, Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, *Supplementary Detailed Reports on Intelligence Activities,* vol. III, 94th Cong., 2d sess. (Washington, DC: U.S. Government Printing Office, 1976).

[17] See Wiretapping Hearings before Subcommittee No. 5. U.S. House of Representatives Judiciary Committee, 84 Cong., 1st sess. 53, 67 (1955), ("1955 Hearings"), 194, 347, 359.

of illegal private wiretapping, by private detectives and others for industrial espionage and in domestic relations matters, and of the ineffectiveness of either Federal or State law to cope with this.

Competing pressures continued throughout the 1960s. The President's Commission on Law Enforcement and the Administration of Justice issued a report in 1967, and near the top of its priorities was organized crime. While it did not explicitly recommend the use of wiretapping, a majority of the Commission members did so. The American Bar Association proposed a statute that became the model for legislation permitting wiretapping that was ultimately enacted in 1968. Because of this activity, the arguments for wiretapping were repeatedly being made and given consideration. For example, Professor G. Robert Blakey, the chief draftsman of the ABA report and proposals and also of the 1968 Wiretap Act, told a congressional committee in 1967:

> The normal criminal situation deals with an incident, a murder, a rape, or a robbery, probably committed by one person. The criminal investigation normally moves from the known crime toward the unknown criminal. This is a sharp contrast to the type of procedures you must use in the investigation of organized crime. Here in many situations you have known criminals but unknown crimes.
>
> So it is necessary to subject the known criminals to surveillance, that is, to monitor their activities. It is necessary to identify their criminal and noncriminal associates; and their areas of operation, both legal and illegal. Strategic intelligence attempts to paint this broad, overall picture of the criminal's activities in order that an investigator can ultimately move in with a specific criminal investigation and prosecution. [18]

The pressures, however, were not all one-sided. In the mid-1960s, illegal tapping and bugging by the FBI, IRS, and others came to light when FBI bugs were accidentally discovered in a Las Vegas gambler's office and in Washington's Sheraton-Carlton Hotel and lawyer-client conversations were overheard. This led to a series of court-ordered revelations of illegal Federal surveillance involving some 50 or more cases. As a result, in 1965 President Lyndon B. Johnson ordered an end to all electronic surveillance except in national security cases. [19]

During this period, the Supreme Court overruled *Olmstead* in *Katz v. United States, 389* U.S. *347 (1967).* The *Katz* decision set out both a general formula for the interests protected by the fourth amendment and specific criteria for a statute authorizing law enforcement wiretapping. [20] The Court's specific criteria for a valid surveillance involved the conventional magistrate's warrant, and the equally conventional probable cause requirements applied to a specific telephone, for a specific need and crime, to the specific suspect conversations and the specific time during which he spoke. The Court also stressed that *prior* notice to the suspect of the interception was unnecessary, and indicated that notice after the interception was constitutionally acceptable. These requirements were drawn from previous related cases and from conventional fourth amendment principles.

All these factors, plus a growing concern about crime, came together to break the 30-year impasse since *Nardone* and produced Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2500ff, which authorizes telephone tapping and microphone surveillance by Federal and State officials, if antecedent judicial approval is obtained. [21] Other than the Foreign Intelligence Surveillance Act in 1978, there has been no significant legislative action since that time, despite a virtual revolution in technology.

---

[18] Hearings on *Controlling Crime Through More Effective Law Enforcement* before the Subcommittee on Criminal Law and Procedures of the Senate Judiciary Committee, 90th Cong., 2d sess. 957-58 (196i'1,

[19] III Church Comm. 298-300.

[20] *Katz* expressly excluded national security surveillance from its discussion. See 389 U.S. at n. 21,

[21] See ch. **2** for a detailed analysis of the statute.

FINDINGS AND POLICY IMPLICATIONS

1. A host of new information technologies has revolutionized the telephone system since 1968—the last time Congress passed major legislation on telephone surveillance by law enforcement agencies and private parties. These technologies include digital transmission and cellular and cordless phones.

Each of the major technological developments affecting the telephone system is discussed briefly below.

Digital Transmission.—Initially, the phone system carried only analog signals over telephone wires. Much of the telephone system in the United States, and especially overseas, is heavily dependent on analog systems, at least for part of a phone call. Increasingly, however, analog voice signals are digitized. The phone system of the future will carry digitized information (voice, data, and image) across wires, optical fibers, microwave radios, and satellite links. The evolution of digital communications, as well as the digital switching devices that enable the system to function smoothly, is beginning to provide expanded services to customers.

The computing and telecommunications industries worldwide are gradually evolving toward a new system, the Integrated Services Digital Network (ISDN), which will allow the transmission of data, voice, image, and video over the same digital system worldwide. The future trend is toward a wholly digitized, efficient, and integrated phone system.[22] Some predict that, in the future, the microphones and speakers in the telephone handset will be the only analog components of the system.[23]

Legal or illegal interception and interpretation of digital signals is not significantly more difficult than for analog signals; the interceptor just needs a coder-decoder and knowledge of the modulation scheme. Digitization of phone calls, thus, does not offer more protection for the content of the call. Transmission over fiber optic lines may offer more protection against illegall interception, to the extent that the operating company can more easily tell when the line has been broken into and where along the line the break has occurred.[24]

Cellular Phones.–The cellular telephone is a technological innovation in providing quality mobile phone service to a large number of customers over an expansive geographic area. The basic technology was first developed at AT&T Bell Labs in the 1950s, and the necessary computer and switching technologies were developed in the 1960s. The critical development was a system that reused frequency spectrum by dividing a service area into "cells." Each cell contains a base station that serves as a radio transmit-receive-switching station. Cellular mobile phone calls are relayed by radio to the base station, which is hooked up to the mobile phone switching office computer. The switching office then routes calls to other base stations or to the telephone network via similar routes. If the call is to another cellular phone it is relayed to the appropriate cell site transmitter. If the party called is using a conventional wire-line phone, then the switching office computer routes it through the telephone system to the receiver.[25]

In 1982, the Federal Communications Commission (FCC) accepted applications for cellular license systems. It received 196 applications for the top 30 markets. The FCC decided to license two types of competitors, a tele-

[22] William Stallings, "The Integrated Services Digital Network," *Datamation*, Dec. 1, 1984, pp. 68-70.

[23] John G. Posa, "Phone Net Going Digital," *High Technology*, May 1983, p. 41.

[24] For trend in fiber optic systems, see Les C. Gunderson and Donald B. Keck, "optical Fibers: Where Light Outperforms Electronics," *Technology Review*, May/June 1983, pp. 33-44; Soichi Kobayashi and Tatsuya Kirnura, "Semiconductor Optical Amplifiers," *IEEE Spectrum*, May 1984, pp. 26-33; Jeff Hecht, "Outlook Brightens for Semiconductor Lasers," *High Technology*, January 1984, pp. 43-50; and Donald B. Keck, "Single-mode Fibers Outperform Multimode Cables," *IEEE Spectrum*, March 1983, pp. 30-37.

[25] "For good descriptions of the technology involved see: Duane L. Huff, "Cellular Radio," *Technology Review*, November/December 1983, pp. 53-62; George R. Cooper and Ray W. Nettleton, "Cellular Mobile Technology: The Great Multiplier," *IEEE Spectrum*, June 1983, pp. 30-37; and Television Digest, Inc., *Cellular Radio–Birth of an Industry, 1983.*

phone company and a radio communications company, in each area. Subsequently, the FCC received almost 400 applications to provide service in the 30 next largest markets and 567 applications to provide service for the next 30 markets.[2e]

Market analysts expect that the demand for cellular service will be large-driven by people who want to communicate while on the move. Cellular phones provide quality communications, and the current high cost will decrease. Some predict that the cost will drop to $500 per phone within 5 years.[27] Service charges started out around $150 per month, but are dropping fast.[28] The technology on which cellular phones are based is capable of providing additional services, e.g., data terminals and printers in a briefcase; public cellular phones on trains, buses, and planes; answering and message services; dictation services; and automatic callback.[29] In addition, encryption devices to protect privacy are now available.

Development of the radiotelephone system has been under way and may be available soon, subject to FCC approval. This system does not need an elaborate transmitter system and would be cheaper than a cellular phone. Radiotelephones can work either as a telephone or as a car-to-car radio. Although radiotelephones have a limited range, users can subscribe to a repeater service that picks up weak signals and rebroadcasts them. Radiotelephones (as well as cellular radios) are subject to eavesdropping. In addition, police scanners that can listen in on personal radiotelephone conversations are now on the market.[30]

Cordless Phones.—The cordless telephone is designed to meet a perceived consumer interest in being able to talk on the phone while walking around the house or in the yard. With the cordless phone, oral messages are no longer transmitted from the receiver to the network via a line, but instead are transmitted between receiver and base station via radio. These transmissions can be picked up accidentally on a home or car radio, and also can be intercepted easily by someone who wants to eavesdrop.

Companies marketing cordless phones and the FCC are well aware of the difficulty in ensuring the privacy of cordless phone calls. The FCC now requires that such phones be labeled with a warning that the conversation may be accidentally overheard. One reason cited for the lack of market interest in cordless phones is that customers desire privacy for their phone calls.

Private Carriers.–Until deregulation of the telephone industry, the market was dominated by common carriers that offered telecommunications services to any potential customer. Because of regulatory restrictions, capital investment requirements, and economies of scale, it was very difficult for an individual or company to set up a phone system. However, deregulation coupled with technological advances now make it possible to set up private telecommunications systems, which serve a specific business or a predetermined group of customers. Parties can also lease dedicated lines from the telephone company or private providers, form local area networks (LANS), and purchase private branch exchanges (PBXs). This variety of phone systems is not reflected in current laws that speak primarily to common carrier systems.

2. The contents of phone conversations that are transmitted in digital form or that are conducted on cellular phones or cordless phones are not clearly protected by existing statutory and constitutional prohibitions on the interception of phone calls.

The major statute prohibiting unauthorized interception of phone calls, Title III of the Omnibus Crime Control and Safe Streets Act, was written at a time when phone calls were transmitted in analog form, over wires maintained by common carriers. The technological changes discussed above have raised a series of questions about the scope of Title III and the possible need for new legislation. The present le-

[26] Huff, op. cit., pp. 59-60.
[27] Television Digest, Inc., op. cit., p. B-8.
[28] Huff, op. cit., p. 60.
[29] Huff, op. cit., p. 61.
[30] Benn Kobb and Lee Greathouse, "Car Radiotelephones Get Personal," *High Technology*, November 1984, pp. 18-21.

gal status of these new technologies is outlined below.

Digital/Data Communications. -Title III covers only the "aural acquisition" of an oral or wire communication, not the acquisition of communication in digitized form or data communications. Recent court rulings have not expanded the scope of Title III to cover digital or data communications. In *United States v. New York Telephone Co.,* 434 U.S. 159 (1977), the Supreme Court held that to be covered by Title III, a communication must be capable of being overheard. In 1978, the Fourth Circuit in *United States v. Seidlitz, 589* F.2d 152, ruled that nonaural communications were not protected by Title III.

Although it is clear that Title III does not cover data communication,[31] there has been some discussion whether Title III would cover phone conversations that are being transmitted in digital form.[32] Most interested parties, e.g., AT&T and the ACLU, now appear satisfied that conversations that are transmitted in digital form are covered by Title III because the interception is still aural and therefore covered by the statute. The Justice Department's position is similar, i.e., the analog-digital distinction is not important and that Title III applies to all phone conversations carried over the wires. Title III focuses not on the method by which communication is transmitted, but on the type of acquisition of that information. Since the Government's interception is aural, it does not matter for Title III purposes whether the transmission was analog or digital or by some other means. However, the courts have not ruled on the coverage of phone conversations carried in digital form and clarification by statute would avoid future legal misinterpretations.

The Foreign Intelligence Surveillance Act of 1978 (FISA) does require a court order for interception of digital conversations. Phone conversations being transmitted in digital form would be protected against unauthorized surveillance if the interception was for intelligence purposes. FISA does not cover law enforcement surveillance.

Section 605 of the Communications Act of 1934 does not provide any protection against unauthorized acquisition of digital wire communications because the courts have ruled that Congress intended Title III to be the exclusive remedy with respect to telephone inperceptions.[33]

Attempts to afford legal protection against the interception of digital or data communications through statutes that prohibit theft are likely to be futile because it is difficult to calculate or prove the informational value taken from the person whose communication is intercepted.

If no statute covers the interception of digital phone conversations, there may still be constitutional protection in the fourth amendment's "expectation of privacy" against unreasonable searches and seizures.

Cellular Telephones.–The issue of whether the interception of cellular phone calls comes under any existing statute, and thus requires some form of court order, has not yet come to the courts. In *United States v. Hall, 488* F.2d 193 (9th Cir. 1973), the Ninth Circuit Court held that Title III protects any communication that is transmitted in part by wire. The Court ruled that a telephone call from a mobile telephone to a landline telephone is protected by the statute, but that a phone call from a mobile telephone to another mobile tele phone is not. The Court characterized this as "an absurd result, " but one required by the statute. Based on the reasoning of the courts in other cases involving radio transmissions (cordless telephones and beepers), Title III and FISA would not apply because the communication was not a wire transmission, and Section 605 would not apply both because of Title III preemption and because cellular telephones use radio, not wire, transmissions. The posi-

[31] In ch. 4, *Electronic Mail Surveillance,* more detailed attention will be given to data communication.

[32] David Burnham, "Loophole in Law Raises Concern About Privacy in Computer Age, " *New York Times,* Dec. 19, 1984, p. A-1.

[33] See: *Watkins v. L. M. Barry& Co., 704* F.2d 577 (5th Cir. 1983) and *United States v. Hall,* 488 F.2d 193 (9th Cir. 1973).

tion of the Justice Department is to secure a Title III warrant before interception because one cannot tell whether the receiver is on a landline phone and hence using telephone wires.

Cordless Telephones.–The status of the protection afforded communication over cordless phones from unauthorized interception is not clear. Two State courts have ruled on the question. In 1984, the Supreme Court of Kansas, in *Kansas v. Howard, 679* P.2d 197, held that the user of a cordless telephone had no fourth amendment "expectation of privacy" and that interception of such communication does not violate Title III. The Court did not address the question of the expectation of privacy of the other party to the conversation. The Rhode Island Supreme Court has recently handed down a similar ruling in *Rhode Island v. Delaurier, 488* A.2d 688 (R.I. 1985). The Justice Department position is that investigatory authorities should get a Title III warrant before intercepting conversations carried over a cordless telephone. It may be important to note that in many instances the information resulted not from the Government actively listening to cordless phone calls, but from neighbors who picked it up on an FM radio dial and turned the information over to Government authorities.

Private Carriers.–Communications carried over private carrier communications systems are not "wire" communications under Title III. In addition, the AT&T consent decree may remove the regional holding companies from the category of common carrier engaged in interstate commerce as defined by Title III, and thus remove these companies from Title III coverage." Given the market trend toward private carrier systems and combination common-private systems, the implications of the current legislative distinction need to be explored for Title III, Sections 605 and 705(a) of the Communications Act, and FCC regulations.

[14]Bruce E. Fein, "Regulating the Interception and Disclosure of Wire, Radio and Oral Communication: A Case Study of Federal Statutory Antiquation, 22 *Harvard Journal on Legislation* **47, 69** (1985).

3. Interception of the content of phone calls represents a substantial threat to civil liberties, but also a significant potential benefit to investigative authorities. This is reflected in the standards and procedures presently embodied in Title III for such interception.

The following discussion uses the framework developed in chapter 2 (see table 6). In terms of the nature of the information acquired, the content of intercepted digitized phone communications is quite specific, detailed, complete, and often of a personal nature. The nature of the information that can be acquired does not vary with the system of transmission, the phone used, or the phone network.

The "private" v. "public" nature of the phone call does not differ at all based on the system of transmission or the phone network employed. It does differ somewhat according to the phone used, in that cellular and cordless phones using radio transmissions are inherently more vulnerable to interception, and thus more public. However, because a communication may be more readily overheard does not necessarily mean that investigative authorities should be able to intercept it with less authorization than for other calls.

The scope of surveillance is the same regardless of the system of transmission, phone used, or phone network employed. In any case, all parties to a phone call are generally overheard.

It is virtually impossible for an individual to detect whether or not the content of a phone call is being intercepted when the interception involves passive reception over the air signals. Again, this is true regardless of the system of transmission, phone used, or phone network employed.

The pre-electronic analogy will most likely be to analog transmission of phone calls made on conventional phones via a common carrier. Such calls are accorded a high level of protection against interception as reflected in Title III.

The governmental investigative interest in intercepting the content of phone calls is quite high. Knowledge of the content of phone calls

would be useful for any type of investigation, at any level of suspicion, and with or without more traditional techniques. As there is a history of policy in this area, extension of protection could arguably be consistent with what now exists.

4. OTA has identified three major options for congressional consideration with respect to policy on interception of the content of telephone calls: a) treat all phone calls similarly from the perspective of the extent of protection against unauthorized interception, i.e., extend Title 111 to cover all phone calls whether analog, digital, cellular, or cordless; b) formulate specific policies depending on the technological constraints and possibilities; and c) do nothing and leave the development of case law to determine policy, depending on individual circumstances.

Each of these options is discussed below in terms of the dimensions developed in chapter 2 (see table 6).

Option A.–The basic rationale for treating all phone calls similarly is that a phone call is a phone call. Therefore, regardless of the system of transmission (digital or analog, wire, satellite, microwave, or fiber optics), the phone used (conventional, cordless, or cellular), and the phone system employed (common carrier or private), phone conversations would be accorded the same protection.

There are two advantages to this approach. The first is that both individuals and investigative authorities would know their rights and responsibilities. A clear policy would disadvantage no one. The second is that the policy incorporates a standard that endures beyond technological changes. If a new type of phone is invented, or a new system for transmission of phone calls, the legal status would be clear to manufacturing companies, customers, investigative authorities, and the courts. Future confusion would be avoided.

Another strong argument for treating all phone calls similarly is that they have been accorded a historical expectation of privacy. Administrative and legislative actions prior to passage of Title III, experience with Title III, and public opinion over time are all supportive of protection for the privacy of phone calls. The analogy here is quite direct.

With respect to the governmental investigative interest involved and the stage of investigation at which it would be appropriate to allow interception, the standards developed in Title III for law enforcement and in FISA for intelligence purposes could be used for all phone calls. The standards for interception of phone calls for purposes of the proper administration of Government programs have not been formulated and are in need of legislative attention.

Option B.–The advantage of formulating specific policy depending on the technology involved is that policy would directly address the peculiarities of each technological situation. Policy would be precise. However, this option has three disadvantages. First, there will necessarily be a period in which there is no policy and in which the temptation will be to wait and see how the technology develops and what marketing is successful. Second, Congress will repeatedly be asked to deal with similar issues on which it will have to build individual hearing records and a separate consensus. Third, if Congress does not act quickly enough, the courts will be called on to set policy.

If this option were chosen, the standards relevant to each technology appear to be as follows:

Digital/Data Communications. -Based on the nature of the technology, the policy principles that exist in case law and legislation, and the investigative practice to date, there appears to be no reason to treat phone communications transmitted in digital form differently from those transmitted in analog form. The preponderance of evidence indicates that data communications are also in need of statutory protection against unauthorized interception. The Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trademarks held hearings on this issue on September 12, 1984. Witnesses from the Justice Department,

AT&T, and the Cellular Communications Industry Association stated the need to develop legislation protecting data communications.

The easiest and most direct policy alternative may be to amend Title III to include data communication. In October 1984, Representative Robert Kastenmeier introduced the Electronic Surveillance Act of 1984, which extended Title III definition of "intercept to include the nonaural acquisition of the contents of such communications. The Kastenmeier bill was reintroduced in the U.S. House of Representatives in September 1985 as the Electronic Communications Privacy Act of 1985 (H.R. 3378). A similar bill (S. 1667) was introduced in the U.S. Senate by Senator Patrick Leahy.

Additionally, it should be noted that computer crime legislation may also affect the security of data and data communications against unauthorized interception.

Cellular and Cordless Phones.– In designing policy for cellular and cordless phones, three separate issues need to be addressed. First, should the content of cellular and cordless phone calls be accorded a lower level of protection because the technology makes it easier to overhear such calls? If the answer is yes, then a standard based on the governmental investigative interest in intercepting such communications and the stage of the investigation needs to be fashioned.

The second issue is whether the caller and receiver should be accorded the same protection. The party using the cellular or cordless phone may know that the conversation can more easily be overheard. The other party most probably assumes that the conversation is via a conventional phone and that the usual protections apply, although under the concepts of one-party consent and assumption of risk, it is possible that the other party may not have a fourth amendment expectation of privacy. The Supreme Court's ruling in *United States v. White, 401* U.S. *745 (197),* that such practices as governmental encouragement and exploitation of misplaced personal confidence does not implicate the fourth amendment's guarantees would also appear to support this. In the Kansas cordless telephone case, the Court held that the user of a cordless phone has no expectation of privacy, but did not discuss the expectation of the other party. Under traditional principles of equity, it is necessary that the expectation of privacy for both parties be established and known in advance.

A third issue relates to the tracking potential of cellular phones. By monitoring the switching of cellular phone calls from one frequency to another, the cellular carrier can determine the location of individuals placing and receiving calls. Moreover, some companies record this information in a computer for billing purposes. At this time, precise locations cannot be determined because the cell sizes are large, but as cellular phones become more popular, cell sizes will be reduced allowing more precise tracking.[35]

The issue of tracking individuals by monitoring cellular phone calls could be dealt with by requiring investigative authorities to get a court order before getting such records from the cellular company. The standards for governmental investigative interest and stage of investigation at which this is considered appropriate would need to be addressed in legislation. Additionally, the legislation could require the cellular carrier to inform potential customers of its policies with respect to customer privacy. The model for such legislation could be the Cable Communications Policy Act.

Private Carriers.-The trend toward private carriers and combined common and private carrier systems throughout the telecommunications field indicates that the legal distinction between common and private carriers may no longer be valid. It appears that the distinction is based on a market configuration that is now outdated. Congress could enact legislation that applies equally to common, private, and hybrid communication systems.

[35] Robert L. Corn, "The Privacy Issue. " *Telocator,* September 1984.

Option C.—To do nothing and leave case law development to determine policy, depending on individual cases, has two serious disadvantages. The first is that, given the universal use of the phone system as a means of communication, lack of clear policy could lead to continued uncertainty and confusion as to the privacy accorded phone calls. The second is that major telecommunications changes are now occurring, and a belated response from Congress could detract from industry stability and growth.

5. New information technologies have also greatly increased the ability to collect and access transactional information about telephone calls, for example, the numbers and places dialed.

Because of the technological sophistication of the phone system, information on the numbers dialed and length of phone calls exists in real time and is stored for billing and administrative purposes. Access to this information makes it possible to determine patterns and interconnections in phone transactions.

Pen Registers.-Pen registers are devices that are attached to a telephone line to record the dialed pulses based on equipment that senses changes in magnetic energy. With a rotary phone call, a very sensitive radio receiver some distance from the wire can also pick up the pulses. Deciphering the numbers dialed by touch-tone phones is somewhat more difficult because the magnetic energy is weaker. Induction coils attached directly to the wire can pick up the signals, but radio receivers cannot.

Pen registers can pick up the number dialed and the length of the phone call. With a reverse phone book, one can then determine the party that was called. In order to install a pen register, one needs the cooperation of the phone company. Each pen register costs about $4,000 to install and monitor, depending on the length of time it is installed.

Automatic Billing Equipment.–With computer-controlled electronic switching systems, it is not necessary to use a pen register to determine calls dialed. Instead, the switch controller can automatically collect information on all calls, toll and flat rate. This can be done for both online data (real time) and for billing purposes. The information is retained on tape and can be accessed when needed.

6. Transactional information about phone calls (e.g., numbers and places dialed) is not clearly protected under existing statutes and judicial precedents on surveillance. Yet access to such information represents a significant threat to civil liberties and a significant potential benefit to investigators.

Title III was directed at the interception of the substance of phone calls and did not address the question of interception of numbers dialed. Transactional information is becoming more valuable as more of it is available and can be cross-referenced.

Pen Registers.–Given the present Supreme Court interpretation of Title III, Government officials do not need a Title III warrant to install pen registers. In 1977, the Court ruled in a 5-4 decision in *United States v. New York Telephone Co.,* 434 U.S. 159, that the FBI did not need a Title 111 warrant to use pen registers because the pen register intercepted nonaural communications and because the legislative history of Title III indicated that Congress intended to exclude pen registers.

Given the present Supreme Court interpretation of the scope of the fourth amendment, an individual cannot claim an expectation of privacy that numbers dialed will remain free from Government interception. The Court reached this ruling in *Smith v. Maryland,* 442 U.S. 735 (1979), in which it argued that Smith assumed the risk that the phone company might reveal all the numbers he dialed.

According to the Justice Department, the Foreign Intelligence Surveillance Act requires that law enforcement officers obtain a court order before using a pen register.[3G] The Justice Department currently requires its investigative departments to obtain a court order before installing a pen register. However, the

[36]John Keeney of the U.S. Department of Justice, Statement Before the Subcommittee on Patents, Copyrights and Trademarks of the Senate Judiciary Committee, Sept. 12, 1984.

court order does not require evidence of a link to illegal activities and does not require judicial review of the reasons for the pen register. Its purpose is to secure the cooperation of the telephone company. The court order generally authorizes the pen register for 30 days. Other Federal agencies appear to follow the Justice Department's guidance on this matter.

Automatic Billing Information.—The information that the telephone company retains for billing purposes and the information that is sent to customers on their bills is currently available to investigative authorities if the company chooses to cooperate in relinquishing the information. The telephone company's position has been that it will not release information without a court order or subpoena. Based on the Court's ruling in United *States v.. Miller,* 425 U.S. 435 (1976), it is difficult to see how an individual could successfully argue that he or she had a privacy interest or property right in this information.

Investigative authorities can generally get billing information from the phone company with a court order or a grand jury subpoena, which does not require probable cause. Recently, the Federal Government announced a plan to monitor long-distance telephone transactions from Federal offices with computer software that can be programmed to select specific information, e.g., phone calls to Dial-a-Joke, Sports Highlights, and Reno, and phone calls over a certain duration or at certain times of the day. The President's Council on Integrity and Efficiency is carrying out this program to reduce the Federal phone bill by discouraging and detecting abuse. " Some have criticized this program because of the possibility that phone calls to congressional offices and news reporters may be monitored as well.

Civil Liberties v. Governmental Interests. In terms of the dimensions introduced in chapter 2 to determine the threat to civil liberties from a particular surveillance technique, the nature of phone transactional information is less personal than the content of phone calls and may, therefore, deserve a lower level of protection. The nature of the information will vary depending on whether it is real-time information, in which case the present location of both parties is also divulged, or historical information. The former would appear to warrant more protection as it is more specific.

With respect to the public or private nature of the communication, transactional information is never considered public information, but rather is proprietary information. Clearly, the phone company needs to keep this information for billing purposes, but this does not put the information in the public realm. The protection accorded transactional information may be less than information that is kept in the home, but it is arguably deserving of a high level of protection.

The scope of surveillance that results from monitoring phone transactions is quite broad in that all phone conversations made are picked up by a pen register or recorded by the phone company. It would be difficult to minimize the scope of the monitoring, unless investigative authorities knew ahead of time the numbers they were interested in or the most likely times that relevant calls would be made,

It is very difficult at present for individuals to detect that their phone transactions are being monitored by investigative authorities. In fact, in order to learn of such monitoring, they would be dependent on the phone company or the Government. It would be fairly easy to give individuals notice of the circumstances under which phone transactional information would be sought and the uses that might be made of it.

In terms of pre-electronic analogies, such transactional information was generally not kept, not kept in detail, and/or not kept in a form that could be easily retrieved. It was, therefore, considered by individuals to be free from monitoring, The closest historical analogy to the monitoring of transactional information for surveillance purposes may be the use of mail covers.

[1] See William Safire, "Thanks for Calling," *New York Times,* Mar. 7, 1985; and Elizabeth Tucker, "U.S. to Eye All Federal Phone Calls," *Washington Post,* Mar. 9, 1985.

Information on phone transactions is potentially of great interest to investigative authorities. The Justice Department and other investigative agencies use such information primarily in the initial investigation of a case to determine whether activities of an implicating nature are occurring. Real-time information on phone transactions is also valuable in determining the location of parties, and is, therefore, valuable at any stage of an investigation. There are no traditional techniques for obtaining this information. A related OTA study on "New Communications Technology: Implications for Privacy and Security" is exploring telephone monitoring issues and policy options in greater depth.

Chapter 4

Electronic Mail Surveillance

Chapter 4

Electronic Mail Surveillance

SUMMARY

The public expects and is provided with a high standard of protection against unauthorized opening of first-class letter mail when in paper form and delivered by the U.S. Postal Service. Constitutional provisions, case law, and postal statutes and regulations collectively provide such protection. However, when mail is sent in electronic form, the existing protections are weak, ambiguous, or nonexistent.

Electronic mail is a relatively recent marriage of computer and communications technology that makes it possible to send, transmit, and receive mail in electronic form. If desired, the electronic output can be printed out in hardcopy and delivered by the USPS or private carrier. But electronic mail also permits terminal-to-terminal communication where the message is never in paper form. Various private companies now offer electronic mail services.

OTA found that there are several discrete stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver:

1. at the terminal or in the electronic files of the sender,
2. while being communicated,
3. in the electronic mailbox of the receiver,
4. when printed into hardcopy before mailing, and
5. when retained in the files of the electronic mail company for administrative purposes.

At each of these stages, OTA found that technological protections vary. Some, like encryption, are still perceived as relatively costly and difficult, though becoming less so. Existing law offers little protection. Portions of the Communications Act of 1934, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Postal Reorganization Act of 1970, and Foreign Intelligence Surveillance Act of 1978 may apply to some portions of the electronic mail process. But overall, electronic mail remains legally as well as technically vulnerable to unauthorized surveillance.

The interception of electronic mail at any stage involves a high level of intrusiveness and a significant threat to civil liberties. The investigative value of intercepting electronic mail will vary. But, traditionally, paper mail has been afforded a high level of protection from interception.

OTA identified three policy options available to Congress:

1. legislate a high level of protection across all stages of the electronic mail process so that electronic mail is afforded the same degree of protection as is presently provided for conventional first class mail;
2. legislate different levels of protection at different electronic mail stages; and
3. do nothing at present, pending further technical and case law developments.

INTRODUCTION

Written communications that are sent between two parties via first class mail receive a high standard of protection against unauthorized opening. This has been well established by both case law, 13x *Parte Jackson* (1877),[1] and postal statutes and regulations. More and more often, however, substantive communications between two or more parties are not written and sealed in an envelope, but are being typed into a computer system and sent by means of telecommunications. The merging of computers and telecommunica-

[1] Upheld the requirement of search warrants as a condition for opening sealed mail. Applied fourth amendment protections on that class of mail for which customers pay a certain rate to send in a sealed envelope or package.

tions opens up many possibilities for faster, cheaper, and more accurate communications. However, it also raises many questions about privacy and the security of such communications against unintentional or intentional tampering.

When electronic mail is being transmitted in data form across wires, it does not come under the purview of either Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which prohibits only aural interception, or Section 605 of the Communications Act of 1934, which prohibits interception of radio transmissions. Interception of digital messages for purposes of learning the contents or altering them is prohibited by the criminal provisions of the Foreign Intelligence Surveillance Act (FISA); however, the scope of such prohibitions is unclear. When electronic mail is in the computer memory of the sender or receiver, there are presently no specific Federal laws prohibiting acquisition of that information, although theft laws may apply as might the Computer Fraud and Abuse Act of 1984 with respect to Federal computers. Moreover, it can be argued that an individual would have a fourth amendment expectation of privacy against Government access to the message. If the message was printed into hardcopy and mailed, then the postal statutes should protect the confidentiality of the message. If the electronic mail company retains a copy of the message for administrative or backup purposes, the individual may have no legal recourse to protect the information from additional access.

BACKGROUND

During the last few years, electronic mail began to develop a significant commercial market. It is expected that market popularity will increase as competition brings prices down and more services and improvements in existing services, especially in the connections between personal computers and electronic mail systems, are offered.[2] The main attraction of electronic mail is that it reduces, if not eliminates, time that is spent in exchanging information over the phone or via the U.S. Postal Service or a courier service. The current adage is that electronic mail eliminates telephone tag. With time, however, the major part of the electronic mail market may be substantive messages, e.g., documents and working papers that would normally be sent through the traditional mail system. Informal messages that would normally be conveyed via phone calls may, in the long run, account for a smaller part of the market.[3]

There are currently a number of providers in the electronic mail marketplace. The U.S. Postal Service (USPS) was an early entrant into the electronic mail market offering two services: E-COM (Electronic Computer-Originated Mail), which was aimed at the domestic business market; and INTELPOST (International Electronic Post), which provides high-speed facsimile service by satellite between the United States and Europe. E-COM has been terminated, and INTELPOST, while still operating, is little used.[4]

Commercial ventures in the electronic mail market have proven more successful and more varied. MCI is now one of the largest electronic mail companies offering both direct computer-to-computer messaging and mixed systems that combine electronic input and transmission with hardcopy output and delivery. One reason MCI can offer inexpensive ef-

[2] *See EMMS Newsletter,* May 1, 1985, p. 1.

[3] David Roman and Stan Writen, "Electronic Mail: Faster Than a Speeding Bulletin," *Computer Decisions,* July 1984, vol. 16, No. 9, pp. 146-160.

[4] See James Bovard, "Zapped by Electronic Mail," *Across the Board,* June 1985, p. 42; House Committee on Government Operations, "Postal Service Electronic Mail: The Price *Still* Isn't Right," House Rep. No. 98-552, 1983; and House Committee on Government Operations, " I NTELPOST: A Postal Service Failure in International Electronic Mail," House Rep. No. 98-675, 1984.

ficient services is that it owns a low-cost, long-distance telephone network.[5] In the spring of 1984, Federal Express entered the electronic mail market with its Zapmail service which provides 2-hour delivery of facsimile copies for up to five pages of text. ITT has targeted its DIALCOM services, including computer-to-computer electronic mail, telex, telegram and courier delivery, into large corporations and the Federal Government. The White House, for example, uses DIALCOM for electronic mail communications with some 22 Federal agencies. GTE Telemail has also been successful in the corporate marketplace. The Source and CompuServe provide an array of computer information services, including electronic mail and various electronic bulletin boards.

As generally used, electronic mail refers to messages that are sent between computer terminals via telephone lines.[6] This does not merely include terminal-to-terminal systems, but also can be interpreted to encompass telegraph, telex, teletext, facsimile, voice mail, and mixed systems that electronically transmit messages, some of which may be subsequently delivered by the postal system or a courier service. A brief description of each of these is presented below:

. Telegraph: A system that transmits one-way electronic messages along circuits within a network of central and branch telegraph offices, where the electronic messages are translated by the receiving operator into typed messages that are hand delivered or telephoned to the recipient.

- Telex: Commonly used for international communications, this telegraph exchange system consists of: a teletypewriter terminal to translate and interpret messages into code; special telegraph circuits designed to carry the code; and a teleprinter to print the communication. Each subscriber is individually issued his or her own telex line and number that a caller dials to send messages that are keyed into the teletypewriter terminal. The message is then transmitted to the receiver's automatic teleprinter. For international telex communications, satellite channels or transoceanic submarine cables are used.

  Current Telex systems, such as the "InfoMaster," can offer delayed message delivery and a multiple address message system, while "FYI News Service" subscribers can receive general news, financial, market, and weather-related bulletins.
- Teletext: This communication system delivers text and graphic messages sequentially in one direction over a television broadcast signal or cable which are then received by a display terminal, like a television set. The receiving terminal exhibits the message on the display screen, and can store or delete the message after viewing. Similar systems that can receive as well as send messages (e.g., home banking or shopping) are known as videotex.
- *Facsimile:* Unlike the telex, this system converts a page of text or images into data. Once the input data is scanned and translated into code, ordinary telephone lines can carry the transmission to a recipient's terminal to be decoded and printed for hardcopy distribution. As an added feature, some facsimile machines, such as the "FaxPak," offer store-and-forward capability.

  A typical facsimile system can transmit a page in 4 to 6 minutes, while more advanced systems can transmit the same amount of information in a few seconds.
- *Voice Mail:* Voice mail is a computer-based system designed to digitize voice from an analog signal for the purposes of relaying short messages or instructions. Like a sophisticated digital phone-answering machine, messages can be stored and forwarded, edited, retrieved, or distributed to a list of users. Future systems are being designed to incorporate options such as voice to text conversion.
- *Electronic Mail:* This computer-based message system can be divided into two categories. In the first, an electronic message is transmitted between two or more

[5] See Bovard, op. cit., p. 46; and Lawrence J. Magid, "Electronically Yours," *PC World,* June 1984, pp. 48-54.

[6] Bovard, op. cit., p. 42.

terminals and remains in an electronic format. In the second, the message is transmitted electronically, but then converted to a hardcopy format to be delivered by traditional mail or courier service. To use a typical electronic mail system, a personal identifier number, password, the recipient's account number, and message are keyed into a terminal. This information is transmitted to a central computer and stored for viewing at the recipient's convenience. Electronic mail systems can send, receive, file, recall, edit, and store textual or graphic messages.

- *Electronic Bulletin Board:* An electronic bulletin board is an electronic mail service (or the equivalent computer-based information service) with a public or private electronic mailbox that is accessible to several persons. A public bulletin board usually is open to many or all subscribers and/or persons with a general password. A private bulletin board is limited to persons with special passwords.

The emergence of electronic mail has raised a number of policy issues, for example: what standards should be used so that competing electronic mail systems can be compatible; should regulations for common carrier systems and private systems be the same or different; and what range of services can or should electronic mail systems offer?[7] Such issues concerning market structure, services, and regulation are beyond the scope of this report. However, issues concerning the security and privacy of electronic mail systems are germane to this study. Indeed, some believe security and privacy issues are critical to the widespread acceptance of electronic mail as a communications medium. The contents of electronic mail communications are of interest to the same parties that are interested in the contents of first-class mail communications. Thus, Government officials might be interested in accessing or maintaining surveillance of electronic mail messages for investigative purposes. Private parties might be interested in electronic mail surveillance for various competitive, personal, and/or criminal purposes.

[7]For discussion of telecommunications and industry structure issues see Raymond R. Panko, "Electronic Mail," *Datamation*, vol. 30, No. 16, Oct. 1, 1984, pp. 118-122; Robert E. Kahn, Albert Vezza, and Alexander P. Roth (eds.), *Electronic Mail and Message Systems–Technical and Policy Perspectives* (Arlington, VA: American Federation of Information Processing Societies, 1981): and issues of *EMMS Newsletter*.

FINDINGS AND POLICY IMPLICATIONS

1. There are at least five discrete stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver: at the terminal or in the electronic files of the sender, while being communicated, in the electronic mailbox of the receiver, when printed into hardcopy, and when retained in the files of the electronic mail company for administrative purposes. Existing law offers little protection.

From a policy perspective, the laws that might be extended or drafted will vary by these five stages because of the historical development of telecommunications and privacy law. Moreover, the technological protections that are available will also depend on the stage of the communications process. Therefore, each stage needs to be analyzed separately to discern policy problems and policy options."

Terminal or Electronic Files of Sender.–At this stage, messages could be intercepted by accessing the computer system of the sender for purposes of reading the message or altering its content. In the case of interception by Government officials, the individual would probably be successful in arguing that he or she had a fourth amendment expectation of privacy in the contents of computer files. Although these are not "papers" in the traditional sense, they are arguably the computer-age equivalent. They are also stored within a

[8]See *ACLU Focus Paper on Electronic Mail*, Jan. 29, 1985, for a similar discussion.

computer file that belongs to the individual, perhaps not in a tangible property sense, but at least in an intangible one, depending on the storage arrangement. If the computer was at home, the individual's expectation of privacy would be greater than if it was an office computer, but use of passwords and access codes would indicate that the individual took precautions at the office to ensure an expectation of privacy. The fourth amendment status of messages held in the computer file of the sender could be clarified by statute. The FBI reported that on the occasions where it has had to acquire information from a data bank, it secured a search warrant as it would have done before going into a residence looking for information.[9]

In the case of private parties accessing electronic mail in the terminal of the sender, there is no specific statute that would protect the confidentiality of the message. At this time, State laws probably offer more protection than Federal laws. Theft laws might apply under some circumstances, although these are framed in terms of physical breaking and entering, and in terms of tangible property. Computer crime laws may also offer some protection against unauthorized private access.

There are also some technical measures that can be adopted to protect the contents of a computer file. Sophisticated password and/or key systems can be used to deter unauthorized access. Audit trails can be developed to detect unauthorized access. Although such systems may not be foolproof, their use will give additional legal weight to someone arguing that their computer mail files are expected to be private.

In Transmission.—At this stage, messages can be intercepted by tapping into the wire over which the message is being sent, breaking into the fiber optic cable, or intercepting satellite or microwave signals. Regardless of the technology used to transmit electronic mail messages, existing law offers little protection against unauthorized interception. Title III of the Omnibus Crime Control and Safe Streets Act would not require Government officials to get a court order before setting up a tap because electronic mail is sent in digital form. Voice mail may be protected under Title III, depending on the interpretation accorded aural communication. (See chapter 3 on telephone surveillance.) Section 605 of the Communications Act of 1934 would not apply unless the electronic mail was being communicated via radio signals, which is rarely the case. Additionally, the purviews of Title III and Section 605 are limited to common carrier communications. Electronic mail systems that use private carriers, e.g., internal company mail systems, would not come under either act. The criminal penalties of the Foreign Intelligence Surveillance Act may prevent Government officials from intercepting digital communications, but it is unclear if these penalties apply to interceptions other than for foreign intelligence purposes.

Again, there are some technical measures that can be used to protect the integrity of a message during transmission. The message can be encrypted using the data encryption standard (DES) or some other code that scrambles or packages the message in a way that makes it difficult to decipher. However, encryption has been expensive and time-consuming on both ends, although costs are dropping.

In the Electronic Mailbox of the Receiver.—At this stage, messages can be intercepted by breaking into the computer terminal of the receiver, if the receiver has one that is used as an electronic mailbox, or into the computer terminal of the electronic mail company where an individual has rented his or her mailbox. In either case, the individual should have a fourth amendment expectation of privacy against Government interception. This expectation will be higher if the mailbox is in the individual's *own* computer terminal, but because renting implies property rights the expectation should also apply if the mailbox is held on the company's terminal. Protection against private party interception would depend on the coverage of theft laws and computer crime laws.

When Printed Into Hardcopy Before Mailing.—Once mailed, the contents of the enve-

[9]Floyd Clarke, remarks at OTA Workshop, May 17, 1985.

lope would receive the same protections that are accorded first class mail. However, there would be no legal protection for the message during the time it was being printed out and before it was put into the envelope. During this time the individual would be dependent on the policy of the electronic mail company and the discretion of its employees.

When Retained by the Electronic Mail Company for Administrative Purposes.-All electronic mail companies retain a copy of the message both for billing purposes and as a convenience in case the customer loses the message. Based on the reasoning in *United States v. Miller, 425* U.S. 435 (1976), where the Court ruled that records of financial transactions, including copies of personal checks, were the property of the bank and that an individual had no legal rights with respect to such records, it is possible that an individual would not have a legal basis from which to challenge an electronic mail company's disclosure of the contents of messages or records of messages sent.

The issue of the privacy of personal information retained by a third party is not unique to electronic mail. It is important to note, however, that access to the administrative files of electronic mail companies can reveal a great deal of information about an individual-the substance of communications, the record of persons communicated with, and the locations of sender and receiver.

The question of the legal status of electronic mail information retained by the company is presently before the courts in a case in which the Government subpoenaed transactional and substantive records of The Source (Source Telecomputing Co.) related to M.V.S. Associates, Inc., Elite Fleet, Inc., and/or Leo Radosta. Leaving aside the questions of the possibly excessive breadth of the subpoenas, the legal question appears to turn on whether The Source is merely the temporary custodian of records, in which case an individual can use fifth amendment protections to prevent disclosure.'" Regardless of what the courts may decide based on the facts in this case, the issue requires attention.

2. The interception of electronic mail at any stage involves a high level of intrusiveness and a significant threat to civil liberties. The investigative value of intercepting electronic mail will vary. But traditionally, paper mail has been afforded a high level of protection from interception.

In order to determine the implications for civil liberties of intercepting electronic mail and the governmental interest in such interception, the electronic mail process as a whole needs to be evaluated in terms of the dimensions developed in chapter 2 (see table 6). This will aid in determining if there is a level of protection against interception that should be guaranteed, regardless of the stage in the process at which the message maybe intercepted.

In terms of the nature of the information, electronic mail surveillance can include both the content of specific exchanges of information, and transactional information concerning the time of the communication and location of the parties. Both types of information may be of a personal nature.

Electronic mail communications generally are intended to be private communications between two parties or among a specified group. The technology employed will allow different degrees of privacy, i.e., personal computer to personal computer communications are inherently more private than electronic mail company to hardcopy delivery communications. Despite the variations in technology, electronic mail communications (including private electronic bulletin boards) usually are intended for private consumption, with the notable exception of public electronic bulletin boards that are open to a broad range of subscribers or users.

In terms of the scope of surveillance, interception of electronic mail communications can be quite broad depending on the extent to which electronic mail is used by a particular individual. Interception of a large volume of electronic mail communications may well be construed as a fishing expedition.

[10] See: *Couch v. United States, 409* U.S. 322 (1973) and *Bellis v. United States, 417* U.S. *85 (1975).*

It is very difficult for an individual to determine if electronic mail has been intercepted, regardless of the stage at which it is intercepted. While in the terminal of the sender or mailbox of the receiver, audit trails and passwords can help in detecting interceptions or attempted interceptions. While being communicated via the telecommunications system, it is virtually impossible for the individual to detect interception. If someone attempts to intercept the message while it is physically being mailed, the post office might detect such an attempt and, if so, might inform the individual. The individual's ability to detect interception of mail while it is retained in the files of the electronic mail company will likewise de penal on the cooperation of the company.

The pre-electronic analogy for electronic mail is probably quite direct—first class mail. Traditionally, first class mail has been accorded a high level of protection from interception.

The governmental interest in intercepting electronic mail will, of course, vary based on the purpose of the investigation, the degree of suspicion, and whether or not other means have been attempted to secure similar information. However, given the high threat to civil liberties posed by interception of electronic mail, it appears that the governmental interest in interception would have to be quite compelling.

3. OTA identified three policy options that are available to Congress. The first would be to legislate a similar level of protection across all stages of the electronic mail process. The second option would be to accord different protections according to perceived differential impacts on civil liberties at particular stages. The third option would be to do nothing.

These three policy options are briefly discussed below.

Option A.–Based on the analogy to conventional first class mail and the level of intrusiveness that interception of electronic mail entails, Congress could provide the same degree of protection for electronic mail that it presently provides for conventional first class mail. Using this as an operating assumption, Congress would need to pass legislation that included the following:

- Prohibition on unauthorized access to an individual's computer file or individual's electronic mailbox unless a court order has been obtained. Two levels of court order may be appropriate. For purposes of intercepting the contents of a file, a court order could be obtained for national security, domestic security, and law enforcement purposes if there is probable cause to believe the individual is implicated in illegal activity. For purposes of determining the transactions the individual engaged in, the requirements for a court order could be the same as for a mail cover (monitoring the names and addresses on the outside of the envelope). The same standards would apply regardless of whether the mailbox was in a personal computer or held by an electronic mail company.
- Prohibition on unauthorized interception of data communication. Although the analogy is still to first class mail, the vehicle for protection is more likely an amendment to Title 11 I that would protect all data communications transmitted over wire.
- Establish the rights of the individual and responsibilities of the company when information is retained by the electronic mail company. The "Subscriber Privacy' provisions of the Cable Communications Policy Act of 1984 may serve as a model. Although it is premature to judge the effectiveness of the "Subscriber Privacy" provisions of this act, comments on the enforcement scheme are in order. In general, the subscriber is dependent on the cable company for information regarding the potential conflicts between the company's practices and the individual's privacy. For example, the company is to inform the subscriber of the uses and disclosure of personally identifiable information. Practically speaking, this may just mean that at the time the individual signs

the contract, he or she is given a sheet of paper containing the company's general policies. The individual may or may not understand, or even read, the information.

The act does place restrictions on the cable company's collection and disclosure of personally identifiable information, but the restrictions are very vague. For example, "A cable operator may disclose such information if the disclosure is necessary to render, or conduct a legitimate business activity related to a cable service or other service provided by the cable operator to the subscriber. " From a surveillance standpoint, the act does require a Government entity to obtain a court order for access to personally identifiable information. The court order must offer evidence that the subscriber "is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case. The individual must be given "the opportunity to appear and contest such entity's claim. "

Option B.—Under this option, Congress could decide that stages one and three (the terminal of sender and electronic mailbox of receiver) should be accorded more protection because they involve places that are more Private and because it would be harder for individuals to detect interceptions unless they were maintaining fairly secure personal computing systems. Congress may not want to take any specific action with respect to the second stage (transmission), but leave it to the resolution of the aural limitation in Title III. Likewise, with respect to interception of information held by the electronic mail company, Congress may wish to treat, in a systematic fashion, all personal information held by third parties.

Option C.–Congress could continue to do nothing at this time and watch the development of the electronic mail market and evaluate case law development. However, there are costs in pursuing this option. The market developments seem clear and the time appears ripe for policy guidance before rights and responsibilities become more confused. Additionally, because of the number of stages at which electronic mail can be intercepted and the range of governmental interests in intercepting electronic mail, the case law development will most likely be very specific to the issues raised in particular cases, and will fall short of a national policy.

Chapter 5

Other Surveillance Issues: Electronic Physical, Electronic Visual, and Electronic Data Base Surveillance

Chapter 5

Other Surveillance Issues

SUMMARY

Electronic Physical Surveillance

Maintaining physical surveillance of individuals is, traditionally, one of the most expensive and risky surveillance techniques used by law enforcement agencies and others. Portable telecommunications devices are now offering a viable substitute in many cases. For example, electronic beepers emit a radio signal that can be monitored in order to track the movements of a car or piece of property to which a beeper is attached. Also, electronic pagers—increasingly used by busy executives, repair personnel, doctors, and the like-can be intercepted to reveal information that may be useful in determining the subject's location and activity.

OTA found that Federal investigative authorities are making extensive use of beepers for conducting electronic physical surveillance of persons and goods, but limited use of paging monitors. OTA also found that legislated policy on beepers and pagers is ambiguous and incomplete, although the U.S. Department of Justice believes that at least some beeper and pager surveillance applications require a search warrant under judicial interpretations of fourth amendment protections.

Based on criteria used to determine the threat to civil liberties-nature of information, nature of place or communication, scope of surveillance, surreptitiousness of surveillance, and pre-electronic analogy-electronic physical surveillance appears to fall somewhere in the middle. The investigative and law enforcement interest appears to be significant-especially for beepers.

OTA identified three options for congressional consideration: 1) legislate one policy for all forms of electronic physical surveillance; 2) formulate separate policies for beepers and pagers; or 3) do nothing at this time.

Electronic Visual Surveillance

Electronic visual surveillance through the use of cameras is an alternative to physical surveillance. In the past, however, the size, cost, and technical requirements of cameras have limited their effectiveness and usefulness. But the latest generation of cameras is smaller, cheaper, and easier to operate. There already is a significant level of video surveillance of public places, such as the use of closed circuit TV in banks, building lobbies, retail stores, and the like. In addition, video surveillance of private places is used for investigative and law enforcement purposes.

OTA found that electronic visual surveillance-whether in public or private places—is not covered by current Federal law, including Title III of the Omnibus Crime Control and Safe Streets Act. The U.S. Department of Justice does voluntarily comply with some provisions of Title III. Even under Department of Justice guidelines, electronic visual surveillance of private places is considered legitimate and does not require a warrant if one party has consented to the surveillance, even if that party is an undercover agent or informer.

Electronic visual surveillance appears to pose a substantial threat to civil liberties, espe cially if conducted in private places and with audio surveillance. The law enforcement interest varies depending on the stage of investigation.

OTA identified five congressional policy options for addressing visual surveillance:

- legislate that such surveillance is prohibited as an unreasonable search under the fourth amendment;
- subject electronic visual surveillance to a higher standard than currently exists

under Title III for bugging and wiretapping;
- treat electronic visual surveillance in the same way as electronic audio surveillance;
- apply a lower standard; and
- do nothing.

Data Base Surveillance

As computerized record systems and data communication linkages become widespread, the potential for computer-based surveillance of the movements and activities of individuals also increases. Various Federal agencies already maintain computerized record systems that could be used as part of a data base surveillance network. Four examples of such systems are: the National Crime Information Center (FBI), Treasury Enforcement Communications System (Treasury), Anti-Smuggling Information System (Immigration and Naturalization Service—INS), and National Automated Immigration Lookout System (INS).

Federal agencies believe that these and other systems are essential to carrying out their authorized responsibilities. However, the systems could include files on any definable category or type of persons, and could be interconnected with numerous other computerized systems.

Based on the results of the Federal Agency Data Request, OTA identified 85 computerized record systems used for law enforcement, investigative, and/or intelligence purposes with, collectively, about 288 million records on 114 million persons. The Departments of Justice and Defense have by far the largest number of systems and records. None of the agencies responding provided statistics on record quality.

Based on a review of technology and policy developments, OTA found that:

- It is technically feasible to have an interconnected electronic network of Federal criminal justice, other civilian, and perhaps even military record systems that would monitor many individual transactions with the Federal Government and be the equivalent of a national data base surveillance system.
- The legal and statutory framework for national computer-based surveillance systems is unclear.
- A central policy issue with respect to computer-based surveillance systems is designing and implementing a mechanism to simultaneously: 1) identify and authorize those applications that have a substantial law enforcement or intelligence value; 2) minimize any adverse impacts on individual rights from authorized use of the systems; and 3) protect against unauthorized and/or expanded use of the systems and the substantial impacts on constitutional rights that might result. Establishment of a data protection board is one option that warrants consideration.
- Other available options, not necessarily mutually exclusive with establishing a data protection board, include: placing data base surveillance applications under Title III of the Omnibus Crime Control Act; requiring congressional approval of specific data base surveillance systems (e.g., by statutory amendment or approval of House and Senate authorizing committees); establishing general statutory standards for surveillance applications; strengthening Office of Management and Budget (OMB) and/or agency oversight roles with respect to data base surveillance; and maintaining the status quo.

PART I: ELECTRONIC PHYSICAL SURVEILLANCE

Introduction

In the past, physical surveillance has generally required around-the-clock agents with backups at various points and has entailed a high risk of detection by the party under surveillance. Monitoring by portable telecommunications devices, or tracking devices, provides a much less conspicuous way of following the physical activities of an individual, a car, or an item, Monitoring by portable telecommunications devices is relatively risk-free in terms of detection. Physical surveillance can be more efficient with the use of portable telecommunications devices. However, electronic tracking may cost more because surveillance can be carried out for a longer period and because of the staff necessary to monitor the information received.

Electronic physical surveillance does raise questions about the rights of individuals under surveillance and the responsibilities of investigative agencies. The availability of new electronic physical surveillance devices to law enforcement agencies is likely to have significant effects on the investigative process. Before the invention of such devices, it was generally assumed that an individual who was engaged in illegal activity was suspicious and was, therefore, aware that someone might be watching. It was also assumed that governmental agents would not invest the resources to watch someone unless they were quite certain that criminal activity would take place. Therefore, it was not thought necessary to legislate restrictions on investigative physical surveillance.

However, these assumptions can no longer be made in an environment that has been changed so dramatically by portable telecommunications devices. It is now easy to attach a beeper to a car or item and follow its movements. Pagers also offer opportunities for monitoring activities. Interception of information destined for pagers that can receive numeric or alphanumeric data could be revealing about the recipient's location or activities. While simple tone-only pagers offer no real surveillance potential, more sophisticated pagers with the ability to receive messages are likely to become commonplace in the next few years. Future paging technology may also be able to function as an electronic mail or data communications terminal. Because of these technological changes, it is necessary to consider whether legislative action is needed to determine when such devices can or should be used for monitoring purposes.

Background

Before analyzing policy issues and policy options, a brief review of the technological development and potential of portable telecommunications devices will be presented to provide a context for the policy discussion.

Pagers

Electronic paging became a possibility in 1949 when the Federal Communications Commission (FCC) allocated three bands of radio frequencies for mobile communications. Those licensed to use these frequencies were considered radio common carriers. Electronic paging did not become popular until the 1960s when the FCC allocated more frequencies, and doctors and traveling salespeople began to use them to stay in touch with the office. In the 1980s, the use of electronic pagers expanded as lawmakers, lobbyists, repair personnel, business executives, and parents began to realize their potential as a means to stay in touch. The number of pagers in use has grown significantly and is expected to increase. In

1976, there were an estimated 424,000 pagers; in 1982, an estimated 2.2 million.[1] Arthur D. Little, Inc., expects that by 1990, 10 million people will carry personal mobile message machines.[2] Arthur D. Little anticipates that public systems will carry 80 percent of paging traffic, and private systems 20 percent.[3]

A number of pagers are available today, and others are in the development stages.[4] Tone-only pagers, which beep or vibrate to inform the wearer to call in, are still the most popular. There are also tone-voice pagers that give the wearer a 12-second voice message. A newly marketed pager uses a 10- or 12-digit liquid crystal to display messages. Such pagers could be used to convey information to the wearer, ranging from phone numbers to stock information to a patient's medical history to a coded message. A device that is presently being developed is the voice-retrieval system for paging. With this pager, the caller's voice message is stored digitally and is retrieved when the subscriber is ready to receive the message. The voice message is broadcast over a regular FM signal or an FM subcarrier signal, as is the case for cellular phones. Another pager in development that is thought to have great market potential is the alphanumeric pager, which displays alphabetical as well as numerical information. Some companies are developing pagers that could print hard copy, thus transforming pagers into pocket data terminals.

As the technology develops, the cost of pagers and the subscription fees are dropping. The size and attractiveness of pagers are also adding to their marketability .-Moreover, the FCC is taking action to expand the market for pagers. Recent FCC decisions will more than quadruple the frequency spectrum available for paging. More paging channels have been allocated to the Private Carrier Paging Service, and paging can also be provided now over FM subcarriers.[5]

A potentially significant effect of recent FCC decisions is the creation of regional and national paging networks. In January 1982, the FCC allocated new frequencies in the 900 MHz band to radio common carriers to develop local and wide-area paging. In May 1982, the FCC set aside one channel at 900 MHz for nationwide paging and two channnels for either regional or national paging, depending on consumer interest. In May 1983, the FCC made all three channels available for nationwide paging. In April 1984, the FCC, on the basis of a lottery, awarded licenses for these three channels. It is expected that a nationwide paging network will be in full operation in 1986.[6] The nationwide networking systems will use satellites and terrestrial phone systems to transmit signals.[7]

Paging radio technology also has enabled the development of automatic vehicle location (AVL) systems. By using the Long Range Navigation system (LORAN-C) of the Department of Transportation, it is possible to locate vehicles based on radio signals sent from the vehicle, to a transmitter, to a base station. With the use of an intelligent modem, information on the location of the vehicle can be communicated to a central points

Beepers

Beepers, also known as "bumper beepers" or "bird dogs, " are electronic transmitters that generate a series of pulses and are used as a tracking device, frequently by law enforcement agencies for covert operations. A series of pulses is transmitted every 2 seconds. Beepers are about 4 inches long and 2 inches

[1] Penny Pagano, "Thousands Heed Beeps From Pagers, " *The Los Angeles Times,* Oct. 20, 1984.

[2] Nell Henderson, "Beepers Said to Link Legions of Area's Workaholics, " *The Washington Post,* Oct. 22, 1984.

[3] Telocator Members Told That Paging to Prosper in the Future," *Telocator Network of America Bulletin,* Sept. 28, 1984.

[4] For a more detailed description of the various pagers and the technology involved see: John G. Posa, "Radio Pagers Expand Horizons, " *High Technology,* March 1983, pp. 44-47, and "Special Report– RCC, " *Broadcasting,* Oct. 4, 1982.

[5] "Telocator Members Told that Paging to Prosper in the Future," op. cit.

[6] "Nationwide Paging, " Information sheet distributed by Telocator Network of America.

[7] F.C.C. Moves Toward National Paging System, " *The New York Times,* Aug. 20, 1984.

"Bob Jane, *'The 'Landsmart' AVI. System, " *Telocator.* August 1983.

wide with a thickness of three-fourths of an inch. Three U-shaped magnets on the bottom of the beeper are covered by a metal "keeper plate" which is sheathed over the magnets when not in use. The metal plate is removed and magnets exposed to attach the beeper to a bumper, underneath a dashboard, or to any metal protrusions. Cars, ships, trucks, and metal containers can be tracked using beepers.

Self-contained batteries supply the power source for beeper transmissions. A remote receiver is used to pick up signals. This receiver can be located in a car, an airplane, or a helicopter, From the air, a helicopter traveling 6,000 feet above the ground can pick up signals within a 250-mile diameter. From the ground in a metropolitan area, a vehicle can pick up signals within a distance of approximately 1 mile.

The beeper receiver can pick up three types of information, The first is directional information that determines the position of a vehicle and the direction it is heading. The second indicates whether a vehicle is stationary or moving. The third involves the relative distance to the vehicle being tracked.

The FCC sets regulations on beeper frequency levels, power ratings, and the like and is involved in the authorization and licensing process for law enforcement use of beepers. The results of the OTA Federal Agency Data Request indicated that 13 Federal agency components currently use beepers, with two other agency components planning such use.

Findings and Policy Implications

1. OTA found that Federal investigative authorities are making extensive use of beepers for conducting electronic physical surveillance of persons and goods, but limited use of paging monitors. Legislated policy for beepers and pagers is ambiguous and incomplete.

The OTA Federal Agency Data Request and discussions with representatives of the Departments of Justice, Treasury, and Defense indicate that investigative authorities are making extensive use of portable telecommunications devices in conducting physical surveillance of persons or goods. Beepers are often attached to vehicles or goods, e.g., shipments of guns, drugs, or materials used in the manufacture of illegal substances. Monitoring of paging devices is not yet a major surveillance technique, in part because they are not thought to be used extensively by persons engaged in illegal activities, except for drug dealers,' and because the geographic range of use is narrow. Both of these features are presently changing. Paging devices would clearly meet the needs of anyone who was trying to make connections to buy or sell goods, or to indicate that a meeting was to take place. Once investigative authorities perceive that paging devices are being used in this way, there will be interest in monitoring them. The development of a nationwide paging system will also make paging devices more attractive to a variety of customers, and also to investigative authorities as a way of monitoring long-distance movements and transactions.

Pagers

Presently, there is no formal executive, legislative, or judicial policy with respect to the interception of pagers for investigative purposes. According to the Justice Department, the protections afforded pagers depend on the type of pager. The interception of "tonal pagers, " emitting only a sound, does not require either a warrantor court order. Title III does not apply because it is not an aural communication; the Foreign Intelligence Surveillance Act (FISA) does not apply because paging is not a data communication. The interception of a display pager is not covered by Title III because it is not an aural interception, but would be covered by FISA because it conveys information in digital form. The Department of Justice's policy is that interception of tonal pagers involves a sufficient invasion of privacy that a court order should be secured prior to interception. Additionally, the Department of Justice believes that users of display pagers have a reasonable expectation of privacy based on the fourth amendment,

"Interview with Maureen Killian, Department of Justice, Sept. 4, 19H5.

and that a search warrant should be obtained under Rule 41 of the Federal Rules of Criminal Procedure. The interception of "tone and voice pagers" would, the Justice Department believes, require a Title III warrant because aural communication is involved.[10]

Beepers

The use of beepers for surveillance purposes has been the subject of two Supreme Court cases. In *United States v. Knotts, 103 S.* Ct. 1081 (1983), the Court ruled that the warrantless monitoring of a beeper was not a search or seizure under the fourth amendment, because there was no reasonable expectation of privacy as the movements being tracked were all public. A year later, in *United States v. Karo, 104 S.* Ct. 3296 (1984), the Court ruled that using a beeper to trail a container into a house and to keep in touch with it inside the house did violate the fourth amendment. The Court found a legitimate expectation of privacy in the house, and what it considered an equally legitimate expectation of privacy that anything coming into a house would do so without a Government surveillance device. The Justice Department policy on the use of beepers follows the Supreme Court's holding, i.e., a warrant is required if a beeper is potentially going to invade someone's privacy. The Department of Justice advises agents to get a warrant for any use of beepers beyond use on a car.[11]

2. Based on the dimensions used to determine the threat to civil liberties as introduced in chapter 2, electronic physical surveillance falls somewhere in the middle. The governmental investigative interest appears to be significant—especially for the use of beepers.

The nature of the information obtained by electronic physical surveillance depends on the device used. The information divulged by portable telecommunications devices varies with the device. Beepers only yield limited information on the location and movements of individuals, cars, or items. Voice pagers and display pagers disclose the content of a message, however brief and cryptic the message might be. Beepers and tonal pagers do not disclose the number of individuals in a location or the activities in which they are engaged.

Electronic physical surveillance does not discriminate between public and private areas, and can be considered intrusive when it allows the monitoring of movements in private areas. Investigative agents who are conducting the monitoring can minimize the intrusion by turning off their devices when parties or objects enter private places.

Electronic physical surveillance casts a narrow net in that it does not involve people who are not specifically under surveillance, unless they are passengers in a car.

It is difficult for an individual to determine whether a beeper has been attached to a car or article. Beepers are easily concealed because of their size. Some may be detected with a metal detector or other sensor; however, one would have to be looking for a beeper in order to find it. It is almost impossible for an individual to detect whether a signal or message that has been transmitted to a pager has been intercepted. It would be relatively easy to warn individuals who subscribe to paging services that the signals and messages received can be monitored by others.

The closest pre-electronic analogy to electronic physical surveillance of public places is physical surveillance on foot or by automobile, while the analogy to surveillance inside private premises is to police undercover work. There has been limited restriction on the use of undercover agents. If they are too aggressive, their case may be dismissed because of entrapment. In general, undercover agents have not been considered an infringement on one's expectation of privacy because an individual is thought to assume the risk of his or her involvement with others. Congress has recently been considering whether such a risk is realistic or if there needs to be some guidance for the types of roles or relationships in which un-

[10] See John Keeney, U.S. Department of Justice, Statement Before the Subcommittee on Patents, Copyrights and Trademarks of the Senate Judiciary Committee, Sept. 12, 1984.

[11] Remarks, Fred Hess, Criminal Division, U.S. Department of Justice, OTA Workshop, May 17, 1985.

dercover agents can engage. Although police undercover work is the closest historical analogy, it may not apply in the same way to electronic physical surveillance because it is based on the assumption of risk. It would be difficult to argue that one assumes the risk that one's movements are always being monitored by a beeper. It would not be as difficult to assume that, if one was carrying a pager, one's activities may be monitored. However, use of pagers may decline if this assumption were widely held.

The governmental interest in using electronic physical surveillance will once again vary with the purpose of the investigation, the degree of suspicion, and whether or not other means have been attempted to secure similar information. Use of beepers and interception of pagers occur in all types of investigations, although they are probably used most often in law enforcement investigations. Electronic physical surveillance is used at all stages of an investigation, but is probably most useful in building a record for probable cause. Electronic physical surveillance is more effective and may be less costly than techniques that are less technologically sophisticated.

The accountability of authorities for use of electronic physical surveillance devices is generally fairly low. They are considered tools of routine investigative use, and can usually be authorized by the agent in the field. If a question of privacy invasion is raised by the use of surveillance devices, then authorization should be obtained from agency headquarters. It is possible to build in a method of accountability, such as authorization by a bureau head for a limited period of time with review and reauthorization possible, and standards of accountability based on the stage of investigation and governmental interest.

3. OTA identified three options for congressional consideration with respect to policy on electronic physical surveillance: a) fashion one policy for all forms of electronic physical surveillance; b) design separate policies for beepers and pagers; and c) do nothing at this time.

Option A.–Fashioning a policy for all forms of electronic physical surveillance is an attractive option in that it is not dependent on specific technological devices and, therefore, will set standards and principles for the future as well as the present. However, given the differences in types of portable telecommunications devices and the different ways in which they are used, it may be difficult to design a comprehensive policy for this area.

Option B.—Although pagers and beepers are similar in that they allow more efficient and less detectable surveillance of physical movements, from a policy perspective they are markedly different in that a beeper needs to be attached by investigative authorities, while a pager is used by an individual. This contributes to the degree of suspicion that an individual has about the possibility of being monitored. People who carry pagers can be made aware of the potential for surveillance that these devices allow. The possibility that one's movements may be monitored by a beeper is more remote for most people. Because of differences in the active involvement of investigative authorities and in the possible awareness of targets of surveillance, it may be necessary to treat beepers and pagers separately. At this time, the differences in the type of information that can be gathered by monitoring beepers and pagers would also seem to dictate separate legislation for each.

It may also be necessary to treat pagers in a discriminate fashion depending on the amount of information that the pager receives. This option would be consistent with the present policy opinion of the Department of Justice.

Option C.–Congress could wait to act until the technology progresses, especially in terms of the development of a nationwide paging network. In formulating legislation for the proper boundaries on police undercover work, Congress may want to consider the parallels between traditional physical surveillance and electronic physical surveillance and design policy that is consistent for both.

PART II: ELECTRONIC VISUAL SURVEILLANCE

Introduction

As cameras have become smaller and easier to activate from a distance, they have become more attractive as a tool for watching people and recording their activities. The evidence that can be obtained from electronic visual surveillance, especially if accompanied by audio surveillance, is as complete as investigative authorities could expect. But there are questions about the intrusive nature of electronic visual surveillance, and the circumstances under which its use is appropriate. Electronic visual surveillance, more than any other form of electronic surveillance, reminds people of the specter of Big Brother watching at all times and in all places.

There is presently a great deal of electronic visual surveillance of public places. Banks have cameras running continuously to monitor both the interior teller counters and also the outside automatic teller machine areas. Airports use electronic visual surveillance in a number of places to ensure the security of the passengers and equipment. Many large department stores, as well as all-night convenience stores, use electronic visual surveillance to deter and detect shoplifting and to compile a visual record of activity. Many cities use closed circuit television to survey street corners in high crime areas, subway platforms, and entrances to public buildings. The Federal Government uses electronic visual surveillance at various Federal buildings to monitor people coming and going. Some employers, especially factory owners and those who maintain large clerical pools, use electronic visual surveillance to monitor the activities of workers.

The motivation for this electronic visual surveillance is a heightened concern for security; the result is that people are becoming more and more accustomed to being watched as they carry out their public life. As cameras become smaller, and easier to install and to monitor, their attractiveness as a means of monitoring activities in private places becomes greater. Previously, one could take actions to ensure an expectation of privacy in a private place, e.g., locking the doors and closing the curtains. But, in the absence of legal standards, the only effective barriers against electronic visual surveillance are the limitations of the technology and such limitations are few.

Electronic visual surveillance of public places is not specifically addressed by Federal statutes, although the assumption is that it is legitimate. Electronic visual surveillance of private places is not presently addressed by Federal laws. The Department of Justice has developed policy guidelines on the use of electronic visual surveillance in private places. These guidelines are regarded as requirements for Department of Justice bureaus (FBI, INS, and DEA) and advisory for other Federal investigatory agencies (Bureau of Alcohol, Tobacco and Firearms and Customs). Electronic visual surveillance of private places where one party has consented to the surveillance, even if that party is an undercover agent or informer, is assumed to be legitimate. The Supreme Court has not ruled on the many questions that are raised by using electronic visual surveillance. For example, if Government agents wish to observe private behavior with the assistance of video cameras or closed-circuit TV, must they get a court order as they would for the use of electronic eavesdropping equipment? Can a court, without specific statutory authority, give authorization for new types of searches or does this overstep the legitimate boundaries of judicial policymaking?

No one has accurate data on the extent of the use of visual surveillance, but there is general agreement inside and outside the investigative community that it is increasing. The Department of Justice has indicated that it has used electronic visual surveillance 18 times in the past year for investigative purposes. Other Federal agencies, such as Treasury and Defense, use video surveillance routinely to monitor the traffic at ports of entry or at buildings containing sensitive materials.

The ease with which video surveillance of private places can be used is in dispute. Some argue that the installation and changing of film make its use prohibitive unless there is easy access to the building or room on a regular basis. For example, video surveillance was used successfully in monitoring the activities of the FALN group in Chicago,[12] but the group met in a "safe house" and thus it was easy for law enforcement agents to gain access. Others argue that the miniaturization of cameras and the use of film that is triggered by activity make it easy to install and maintain video equipment. In support, they cite numerous technological developments and an R&D trend that indicates cameras and film will become more attractive for investigative purposes.

Electronic visual surveillance of private places is most often used when one party consents to the surveillance and can either install and monitor the camera or make it possible for others to do so. Under this circumstance, no Title III warrant or judicial intervention is necessary. However, such enhancement of what an undercover agent or informer can witness and testify to may be significantly more intrusive than an agent acting alone, and on that basis might be required to have some form of judicial authorization.

Background

Before analyzing policy issues and policy options, a review of electronic visual surveillance developments will be presented to provide a context for the policy discussion.

The early literature on modern surveillance techniques warned of the great potential offered by hidden television and video cameras. [13] In the 1960s, this was viewed as a threat rather than a reality because the size and sophistication of cameras made it difficult to install, conceal, and maintain them for surveillance purposes. A number of developments have eliminated such problems. [14]

Miniature television cameras equipped with a "charge-coupled device' rather than the traditional bulky television tubes are widely available at reasonable prices. Closed-circuit cameras also make use of this technology and thus can be easily installed. Technological advances have refined the sensor in the charge-coupled device and have made it even smaller and more powerful. It is predicted that miniature cameras will soon be on the market. These cameras could be concealed in anything from a briefcase, to a lamp, to a plant. It would thus be easy for an agent who has even brief access to an area under surveillance to install a miniature camera, leave, and return later to retrieve the film.

Fiber optics also permits the concealment of small cameras with the lens located at the surveillance site and the camera located at a distance. This is possible because of a "light pipe, " a bundle of thin, transparent fibers, which conducts light and visual images from a lens to a camera. With these devices, an agent need only enter the premises once, to install the lens; film changing and retrieval can be done at a distance.

Low light level television technology makes it possible to see in the dark. Such devices have been used in several cities to detect street crime. Infrared television cameras also make it possible to see in the dark by detecting infrared radiation with a camera that *is* sensitive to such radiation or by detecting infrared radiation and converting it to electrical images. The systems can then produce a detailed black and white picture.

The major advance in the area of visual technology in the 1980s is the development of machine vision systems. Such systems combine video and computer technologies to allow computerized analysis of what is being captured

[12] See *United States v. Torres* (**No. 84-1077,** decided Dec. 19, 1984).

[13] See: Alan Westin, *Privacy and Freedom* (New York: *A theneum*, 1967) and Samuel Dash, R. F, Schwartz and Robert Knowlton, *The Eavesdroppers {New* York: Da Cape, 1959).

[14] For a review of the technologies available in the mid-1970s see: David P, Hodges, "Electronic Visual Surveillance and the Fourth Amendment: The Arrival of Big Brother'?" 3 *Hastings Constitutional Law Quarterly* 261 (1976).

on the camera. Both the computer hardware, which allows the system to rapidly scan and pick up the coordinates that define the outline of images,[15] and the software, which is derived from artificial intelligence research and enables images to be scanned in relation to preprogrammed patterns, 'G are important to the effectiveness of machine vision systems. Such systems have been used primarily in industry to perform a number of labor-intensive inspection tasks, including: identifying shapes, measuring distances, gauging sizes, determining orientation, quantifying motion, and detecting surface shading.[17]

Although the major market for machine vision systems is thought to be factories, there are other areas in which labor-intensive analysis of films could be done by these systems. '8 One is in defense for verification of treaties or evaluation of reconnaissance films from satellites. [19]Another is in the investigative area where films that are captured through electronic visual surveillance are then analyzed by machine vision systems to differentiate the segments of the film that are relevant to an investigation from those that are not. Use of machine vision systems would drastically reduce what is presently a very labor-intensive part of electronic visual surveillance, and thus might make it more attractive.

Findings and Policy Implications

1. OTA found that electronic visual surveillance is not currently covered by Title III of the Omnibus Crime Control and Safe Streets Act. The U.S. Department of Justice voluntarily complies with some Title III provisions. Some judges have asked for, congressional clarification.

"Marsha Johnston Fisher, "Micro-Based 'Roving' Eye Sifts Motion, " *MISWeek*, Nov. 14, 1984, pp. 1, 42.

[16]Paul Kinnuean, "Machines That See, " *Technology}*, April 1983, pp. 30-36.

'-tJohn Meyer, ''Vision Systems: Technology of the Future at Work Today, " *Computerworld*, May 27, 1985, p. 13.

[18]See: Edith Myhers, "Machines That See, " *Datamation*, Nov. 1983, pp. 90-103, and ''Machine Vision Merges With Process Imaging, " *Electronic Market Trends*, February 1985, pp. 17-19.

"'Da \ 'id Hafemeister, ''Advances In Verification Technology, " Bulletin of the Atomic Scientists, January 1985, pp. 35-40.

The courts have upheld the use of video surveillance for law enforcement purposes in a number of cases. In evaluating the appropriateness of video surveillance, judges have considered the place under surveillance, the evidence already accumulated, and the warrant process used.

In 1981, the Court of Appeals of New York, in *People v. Teicher, 439 N.Y. S.* 2d 846, upheld the use of video surveillance in a case where a dentist was charged with sexually abusing his patients. The judge ruled that the warrant authorizing video surveillance was valid because probable cause was clearly established by the affidavit, the warrant described the place to be searched and things to be seized, the warrant explicitly provided that surveillance be conducted in such a way as to minimize coverage of activities not related to specified crimes, and the warrant gave evidence that there were no less intrusive means for obtaining needed evidence.

In 1981, the Michigan Court of Appeals in *People v. Dezek*, 308 N.W. 2d 652, ruled that a warrant for video surveillance of a restroom in a highway rest area where homosexual activity was suspected was invalid because it did not limit the search to precise and discriminate circumstances.

In December 1984, the Seventh Circuit Court of Appeals handed down the major decision to date on the question of video surveillance, *United States v. Torres.* At issue was the FBI's video surveillance of the Puerto Rican nationalist group FALN for more than 130 hours over 6 months. The Seventh Circuit, in an opinion authored by Judge Richard Posner, held that the courts could authorize electronic video surveillance if they followed the requirements of the fourth amendment's warrant clause, i.e., "no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. " In this case, the Government asked for the warrants in conjunction with its application for Title III eavesdropping warrants and followed the Title III requirements. The Court held that:

> A warrant for video surveillance that complies with those provisions that Congress put into Title III in order to implement the fourth amendment ought to satisfy the fourth amendment's requirement of particularity as applied to such surveillance.[20]

The Court went onto state that it did not suggest that compliance with Title III was necessarily required, but said that "we would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope. "[21] It is important to note that Judge Posner did not include all of the Title III requirements, i.e., the exclusionary rule, the limitations on which Federal officials could make an application, limits on the severity of the crimes that could be involved, and limits on State and local use.[22]

The Department of Justice policy is to require a warrant analogous to a Title III warrant for electronic visual surveillance that is not in a public place or that is conducted in a nonconsensual situation. The policy is the result of a desire to have evidence as clean as possible, and the view that it is better to get a warrant "just in case" rather than have a judge rule the results of electronic visual surveillance inadmissible at a later date. The Department of the Treasury reports that it follows the Department of Justice guidelines for use of electronic visual surveillance.[23]

Although the present Department of Justice guidelines require a warrant analogous to a Title III warrant for electronic visual surveillance, the Attorney General has delegated the authority to authorize television surveillance to a responsible official within the Criminal Division who may authorize the surveillance if he or she:

> . . . concludes that the proposed surveillance would not intrude on the subject's justifiable expectation of privacy . . . If such official concludes-that the surveillance would infringe on the subject's justifiable expectations of privacy, he shall initiate proceedings to obtain a judicial warrant.[24]

In the case of electronic visual surveillance of public places or places to which the public has unrestricted access, the head of each Department of Justice investigative division has responsibility for issuing guidelines for that division.

In 1984, Representative Robert Kastenmeier introduced the Electronic Surveillance Act of 1984 which, in part, would bring video surveillance under the Title III warrant requirements. In this bill, video surveillance is defined as "the recording of visual images of individuals by television, film, videotape, or other similar method, in a location not open to the general public and without the consent of that individual. '[25] In September 1985, Congressman Kastenmeier introduced a separate bill, the Video Surveillance Act of 1985 that deals exclusively with video surveillance.[2G] Other electronic surveillance activities are covered in the Electronic Communications Privacy Act of 1985, also introduced in September 1985.[27]

2. Electronic visual surveillance appears to pose a substantial threat to civil liberties, especially if conducted in private places and with audio (as well as video). The governmental interest varies depending on the stage of the investigation in which electronic visual surveillance is to be used.

Before examining specific policy options, it is useful to examine the policy implications of electronic visual surveillance in light of the principles that appear to have guided surveillance policy to date. Based on the dimensions introduced in chapter 2, electronic visual surveillance, especially when used in conjunction

'{'United *States v. Torres*, No. 84-1077, p. 17 (7th Cir., Dec. 19, 1984).

[21] Id, at 19.

[22] Remarks made at OTA Workshop, May 17, 1985.

[23] Remarks made at OTA Workshop, May 17, 1985. "Department of Justice, Order No. 985-82, "Delegation of Authority to Authorize Television Surveillance. "

[25] H.R. 6343, sec. 8, 3117, c.

[26] See H.R. 3455, Video Surveillance Act of 1985 and U.S. Congress, House of Representatives, Congressional *Record*, Extension of Remarks, Sept. 30, 1985, p. E-4269.

[27] See H.R. 3378 and S. 1667, Electronic Communications Privacy Act of 1985; U.S. Congress, House of Representatives, *Congressional Record*, Extension of Remarks, Sept. 19, 1985, p. E-4128; and U.S. Congress, Senate, Congressional *Record*, Sept. 19, 1985, p. S-11795.

with audio surveillance, poses a great, if not the greatest, threat to civil liberties.

The nature of the information that is gained with electronic visual surveillance is very personal. The information is quite complete, including the content of movements, facial expressions, and nonverbal communications, as well as conversations if audio is used.

Video surveillance can be usefully applied to surveillance of any area. The present controversy is focused on the surveillance of private places. Electronic video surveillance is capable of penetrating the most private places, where curtains are drawn and doors are locked, without leaving a trail.

The scope of a video or closed circuit TV camera is broad. All persons and activities that come in camera range will be filmed. Depending on the area under surveillance, it is likely that a number of people unrelated to the investigation will be covered. In this case, the more private the area to be monitored, the narrower the scope of the surveillance. The scope of the surveillance might be minimized by the use of machine vision systems that could scan the film for the targets of the surveillance or for certain types of motions.

Given the miniaturization of video and TV cameras, it is very difficult for an individual to detect electronic visual surveillance. Again, one would have to suspect that he or she was the target of an investigation and would have to look carefully to locate a hidden camera. Additionally, the present policy of allowing electronic visual surveillance without a warrant if one party has consented raises very serious questions about how the concept of assumption of risk is applied.

The historical analogy would be to undercover agents, although the use of video surveillance is much more powerful in terms of detail and unimpeachability. While the testimony of an agent or informer could always be questioned and needs corroboration, the film would probably be accepted. It is always possible, however, to edit a film to make it more incriminating and some editing may not be detectable.

The governmental interest in using electronic visual surveillance will vary. Video surveillance would be useful in investigations for any purpose, but, given the threats to civil liberties involved, would probably be difficult to justify for investigations to ensure the proper administration of Government programs and investigations of minor felonies and misdemeanors. Given the difficulties of installing and monitoring and the need to have certain basic information, electronic visual surveillance will most likely be used when there is a high level of suspicion. As it is such an intrusive form of surveillance, it would be very hard to justify its use during the early stages of an investigation. Although electronic visual surveillance is more effective and less costly than less technologically sophisticated techniques, the threat to civil liberties involved would seem to require that other techniques be tried first.

The present rules on the accountability of authorities using electronic visual surveillance are not clear. The Department of Justice guidelines appear to leave officials in the Criminal Division some discretion, in that they have to determine if the surveillance would violate an expectation of privacy and hence require a court warrant. Also unclear is the definition of a public place.

3. OTA identified five policy options for addressing electronic visual surveillance—ranging from prohibiting such surveillance as unconstitutional to doing nothing. In formulating policy, the issues of consensual v. nonconsensual visual surveillance and surveillance of public v. private places need to be given careful consideration.

The five policy options are discussed below.

Option A.–The first option is to legislate a prohibition on electronic visual surveillance be cause Congress considers it an unreasonable search under the fourth amendment. The basis for choosing this policy option might be the assumption or belief that electronic visual surveillance is an inherently unacceptable form of surveillance because: 1) the information it secures is so complete and specific; 2) it can pick up the most private activities in hereto-

fore private places; 3) it captures the activities of people not under investigation; 4) it captures the unrelated activities of the targets; 5) it is very difficult to detect, and 6) its pre-electronic analogy, i.e., undercover agents, is also regarded as intrusive.

Option B.—The second policy option is to regard electronic visual surveillance as more intrusive and invasive than eavesdropping, but not unacceptable in all circumstances. The legislative option then would be to subject electronic visual surveillance to higher authorization standards than exist for bugging and wiretapping under Title III. This option would be especially applicable in four areas. First, new minimization standards or a new concept to restrict the scope of the invasion, in terms of both place and content, might be developed. Additionally, the list of crimes and circumstances for which electronic visual surveillance is considered appropriate might be developed independently of the list for wiretapping. Third, the use of video surveillance might be restricted to only very sensitive and important types of investigations. Lastly, documented exhaustion of other techniques might be required.

Option C.–The third policy option would be to treat electronic visual surveillance in the same way as electronic audio surveillance. The advantages of this are that visual surveillance is generally conducted with audio surveillance so that only one warrant would be necessary, and that Title III is a known and tested procedure. The disadvantage is that the use of both audio and video may pose a greater risk to civil liberties.

Option D.–The fourth policy option would be to apply a lower standard to electronic visual surveillance than to eavesdropping. This would be hard to justify, given the principles that appear to govern the use of surveillance. It could only be justified if video surveillance were being used alone.

Option E.–The fifth option would be to do nothing. The disadvantage of this option is that both Judge Posner's request to Congress to deal with the issue and the questions raised with the existing Department of Justice guidelines would remain unanswered in terms of legislated policy.

PART III: DATA BASE SURVEILLANCE

Introduction

A significant implication of widespread computerized record systems and data communication linkages is the increased potential for computer-based surveillance of the movements and activities of individuals.

In modern society, most persons leave a trail of transactions with various institutions—governmental, retail, financial, educational, professional, criminal justice, and others. Before the widespread use of computer-communication systems, linking various kinds of transactions was very difficult, if not impossible, since transactions were paper based and the cost of matching or linking paper records was prohibitive. In addition, the time delay inherent in paper linkages would negate much of the potential surveillance value.

Computer-based record systems and electronic linkages make it possible to overcome the cost and time barriers associated with paper systems. In theory, the technology permits the instantaneous linkage of a large number of record systems that would capture and consolidate, for example, gasoline credit card transactions, telephone calls, retail credit card transactions, bank card transactions, and transactions with Government agencies. Thus, electronic linkages could be used to conduct surveillance of individuals who are of investigative, law enforcement, and/or intelligence

interest to the Government. This assumes, of course, that the Government agencies would have electronic access to transactional record information.

Background

One example of a Federal computerized record system that could be used for surveillance purposes is the FBI's National Crime Information Center. NCIC maintains an "electronic bulletin board" of, among other things, wanted persons, missing persons, and persons with criminal history records. Law enforcement and criminal justice agencies make electronic inquiries to the bulletin board to ascertain whether particular individuals are listed as wanted or missing or have a prior criminal record.[26] The process of making inquiries about specific persons also generates information about the location and movement of these individuals and, indirectly by followup with the inquiring officials, more detailed information about the nature of a person's activities at a given point in time.

NCIC is, in effect, a computer-based system for locating persons who are listed as wanted or missing or have a prior criminal record. Until 1982, with one exception, NCIC was not used for intelligence purposes, that is, for locating individuals not having a formal warrant outstanding and/or a formal criminal record. The one exception was during the the early 1970s, when the FBI made very limited use of NCIC to keep track of, for example, bank robbery suspects. The objective here was "to enable law enforcement agencies to locate, through NCIC, individuals being sought for law enforcement purposes who did not meet the criteria for inclusion in the NCIC wanted person file. "[29] In other words, NCIC was being used to track individuals who had not been formally charged with a crime and did not have an outstanding warrant for a Federal offense or other extraditable felony or misdemeanor offense.

The early 1970s (actually April 1971 to February 1974) pilot project had not been authorized by Congress. From then until 1982, the FBI rejected all requests or proposals for intelligence use of NCIC. However, in 1982 the Department of Justice and FBI approved a U.S. Secret Service proposal to establish an NCIC file on persons judged to represent a potential threat to Secret Service protectees. That Secret Service file is now fully operational, and includes the names of about 125 persons judged by the Secret Service to represent substantial threats. Apparently, according to FBI Director William Webster, the file has been quite useful in helping the Secret Service to keep track of (i.e., maintain surveillance on) the location and movement of a significant number of these persons.[30]

During the past 2 years, several other proposals for intelligence use of NCIC have been discussed, although none has been approved. For example, suggestions have been made to add new NCIC files on white-collar crime suspects and suspected organized crime associates.

Beyond this, the already existing electronic linkages between NCIC and other Federal law enforcement communication systems (e.g., the Treasury Enforcement Communication System, or TECS) easily could be extended to other Federal criminal justice record systems and even to Federal noncriminal justice record systems.

TECS is a good example of the extensive electronic linkages already in place. TECS includes a wide range of information on persons that are suspected of or wanted for violations of U.S. Customs or related laws, including persons suspected of or wanted for thefts from international commerce, and persons with outstanding Federal or State warrants. TECS includes the same kind of information on sus-

[28] For further discussion of NCIC, see OTA, *Assessment of Alternatives for a National Computerized Criminal History System*, October 1982.

[29] Letter from Harold R. Tyler, Jr., Deputy Attorney General, U.S. Department of Justice, to Senator John Tunney, Chairman, Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, Oct. 29, 1975.

[30] Statement of William Webster, FBI Director, at Oct. 17, 1984, NCIC Advisory Policy Board Meeting.

pects that has proven so controversial when proposed for NCIC. Of course, TECS is not accessible on-line to tens of thousands of State and local law enforcement and criminal justice agencies, as is NCIC. Nonetheless, TECS is accessible to numerous Federal agencies (plus two foreign agencies), as indicated in table 7.

The so-called Border Enforcement System is the major component of TECS. Computerized information from this system is used, among other things, to: assist U.S. Customs and the Immigration and Naturalization Service personnel screen persons and property entering and exiting the United States; alert Customs and INS officers to potentially dangerous persons or situations; provide investigative data to Customs or other agency law enforcement or intelligence officers; and aid in the exchange of data with other Federal, State, or local law enforcement agencies.

As of May 1, 1985, the TECS Border Enforcement System included computerized records on over 2 million persons. Table 8 gives the distribution of the record sources.

One of the TECS users and record sources is INS. INS, in turn, has its own extensive computerized law enforcement, investigative, and intelligence systems, with records on, collectively, several tens of millions of persons. Highlights of several of the INS computerized record systems are presented in table 9.

Again, two of these systems–Anti-Smuggling Information System and National Automated Immigration Lookout System—include information on suspected as well as known violators. And one of the major purposes of these two systems is to monitor the movements of suspected violators.

Other Federal agencies maintain similar computerized record systems. Based on the results of the Federal Agency Data Request, OTA identified 85 computerized record systems operated by Federal agencies for law enforcement, investigative, and/or intelligence purposes. Out of 142 agency components responding, 36 (or 25 percent) reported the use of at least one such computerized system. Collectively, the 85 systems include about 288 million records on about 114 million persons. (Note that some systems may overlap with multiple records on the same persons, and some agencies did not know or did not provide the number of records and persons per system. Nonetheless, the overall results provide the most complete accounting of such systems to date.) The Departments of Justice and Defense have by far the largest number of systems and records. Justice reports 15 systems with, collectively, about 241 million records on 87 million persons. Defense reports 18 systems with about 29 million records on 22 million persons.

Table 7.—Treasury Enforcement Communication System/ Border Enforcement ,System Users

- U.S. Customs Service
- Bureau of Alcohol, Tobacco and Firearms
- Immigration and Naturalization Service
- Federal Bureau of Investigation
- U S. Marshals Service
- Interpol (International Police Organization)
- Drug Enforcement Administration
- El Paso Intelligence Center
- Internal Revenue Service
- U.S. Coast Guard
- U.S. Department of State
- National Narcotics Border Interdiction System
- Royal Canadian Mounted Police

SOURCC U S Customs

Table 8.—Source of Treasury Enforcement Communication System/Border Enforcement System Records

Source	Number of records
U.S. Customs Service	897,963
Immigration and Naturalization Service	32,828
National Narcotics Border Interdiction System	959
National Crime Information Center	220,693
U.S. Coast Guard	2
Internal Revenue Service Inspection	6,102
Internal Revenue Service Criminal Investigation	100,692
Drug Enforcement Administration	114,387
Bureau of Alcohol, Tobacco and Firearms	712,720
Royal Canadian Mounted Police	22,022
U.S. Department of State	19,721
Interpol	49,699
Total	2,177,788 records (on 2,153,888 person)

SOURCE U S Customs as of May 1 1985

Table 9.—Selected INS Computerized Record Systems

Name of record system	Contents	Number of records	Number of persons
Anti-Smuggling Information System (ASIS)	Known or suspected alien smuggling operations	750,000	unknown
Central Index System (CIS)	All aliens and naturalized citizens except temporary visitors	152,000,000	21,000,000
Non-Immigrant Information System (NIIS)	All temporary visitors to U.S.	24,000,000	24,000,000
Student School System (STSC)	All foreign students and schools they attend	*750,000*[a]	687,000
National Automated Immigration Lookout System (NAILS)	Known or suspected violators of INS laws and other Federal statutes	*40,000*	*40,000*

[a]87,000 persons plus 18,500 schools

SOURCE Immigration and Natural ization Service, based on June 1985 response to OTA Federal Agency Data Request

OTA also asked agencies for any statistics on record quality (completeness and accuracy) for such systems. No such statistics were provided by any of the 142 agency components responding. The four specific examples noted earlier illustrate the already extensive development of computerized data base systems operated by Federal agencies for law enforcement, investigative, and/or intelligence purposes. Federal agencies believe that these systems are essential to carrying out their authorized responsibilities. However, the systems are capable of including files on any definable category or type of persons, and are capable of interconnection with numerous other computerized systems. As a result, these systems (and others like them) provide the technical infrastructure of a data base surveillance system.

Findings and Policy Implications

1. It is technically feasible to have an interconnected electronic network of Federal criminal justice, **other civilian, and perhaps even military record systems that would monitor many individual transactions with the Federal Government and be the equivalent of a national data base surveillance system.**

For example, the current Secret Service file on NCIC could be extended so that the list of dangerous persons would be checked against not only NCIC wanted person and criminal history inquiries, but also social security, food stamp, and other kinds of inquiries or record transactions that would indicate the location or activities of listed persons. This scenario could be further extended to include travel and credit card transactions and the like.

Of course, these are hypothetical examples at this point in time, but serve to demonstrate the vast technical potential for computer-based surveillance inherent in record linkages among computerized systems. These kinds of potential applications raise numerous issues, ranging from whether the application would be cost effective and serve a significant, useful, and lawful criminal justice purpose to the possible implications for civil and constitutional rights.

For example, first amendment rights could be violated to the extent a national computer-based surveillance system was used to monitor the lawful and peaceful activities or associations of citizens or if it were to have the effect of discouraging such activities or associations. Fourth amendment rights could be violated if the surveillance amounted to an unreasonable search and seizure of personal information. And, as a final example, fifth amendment rights to due process could be violated if such surveillance was conducted without first establishing probable cause or reasonable suspicion and without serving advance notice on the subject individual.

The possible civil liberties implications would need to be balanced against the Government's interest in, for example, enforcing public laws, maintaining social order, and protecting the national security. Thus, the trade-offs could, indeed, be difficult to balance.

2. The legal and statutory framework for national computer-based surveillance systems is unclear.

The systems would appear to be subject to the Privacy Act and perhaps other statutes, depending on the purpose. Law enforcement investigative record systems are exempt from key elements of the Privacy Act, but other record systems would have to establish that surveillance use is a routine use under the Privacy Act, and all such systems would have to publish notices in the Federal Register and withstand the inevitable congressional scrutiny. This would appear to be quite difficult to do, although computer matching was defined as a routine use, apparently with relatively little difficulty. On the other hand, if the surveillance was directed at, say, foreign terrorist activity, the system might fall under Foreign Intelligence Surveillance Act and be subject to little or no public scrutiny. Data base surveillance does not appear to fall under Title III of the Omnibus Crime Control and Safe Streets Act since there would be no "aural" acquisition.

3. A central policy issue with respect to computer-based surveillance systems is designing and implementing a mechanism to simultaneously: 1) identify and authorize those applications that have a substantial law enforcement or intelligence value; 2) minimize any adverse impacts on individual rights from authorized and/or expanded use of the systems and the substantial impacts on constitutional rights that might result. Establishment of a data protection board is one option that warrants consideration.

One policy option that has been proposed from time to time in the United States and has been implemented in other countries is a data protection board. Such a board was proposed in the 1970s with respect to NCIC, and in particular the computerized criminal history **(CCH)** program As early as September 1970, OMB recommended the establishment of a strong "policy control board' that would report directly to the U.S. Attorney General. The board was to include officials from the FBI, the Law Enforcement Assistance Administration (LEAA), and the States, and represent all elements of the criminal justice community. Comprehensive legislative proposals developed in 1974 included an independent Federal Information Systems Board that was to be responsible for the operation and regulation of a national CCH system. On a broader level, several European countries have established independent data protection boards or authorities that have some oversight authority over law enforcement and intelligence systems, as well as a wide range of privacy-related systems (e.g., social services, health, and education).

The institutional placement of such a board or authority would be important. If it were to be a new board within an existing department, its power might be too dependent on that of the department and its character shaped by that department. Additionally, the department might well have interests that might conflict or interfere with the responsibilities of the board. If it were to be a board reporting to the President, it would have added stature and potential influence, but it might easily be politicized, and its visibility and stature might well change with changes in administrations. If the board were to report to Congress, either directly or through a special joint committee, it would be independent of the executive agencies that have stakes in personal information collection and use. It might be less open to partisan uses, but the board might become too removed from the realities of agency operations.

The responsibilities of such a board or authority are also important. Should the board's jurisdiction be limited to some surveillance applications, all surveillance applications, all law enforcement/intelligence uses, privacy-related applications, and so forth? The broader the responsibilities, the larger the necessary size and budget of the board, or, in the absence of adequate resources, the greater the work overload. On the other hand, a broad mandate may be necessary to gain the necessary political support, thus contributing to a better overall understanding of agency technologies and practices and resulting in more effective oversight and better decisions.

Other questions include the size and composition of the board, process of appointments, scope of authority, and extent of decisionmaking v. advisory, research, and/or information clearinghouse responsibilities.

4. Other available options, not necessarily mutually exclusive with establishing a data protection board, include: placing data base surveillance applications under Title III of the Omnibus Crime Control Act; requiring congressional approval of specific data base surveillance systems (e.g., by statutory amendment or approval of House and Senate authorizing committees); establishing general statutory standards for surveillance applications; maintaining the status quo; and strengthening OMB and/or agency roles with respect to data base surveillance.

One congressional option would be to amend Title III, making data base surveillance subject to the Title III procedural and balancing requirements. Another legislative option would be to amend the enabling statutes of the various individual computerized systems that are or could be used for surveillance purposes (or enact specific enabling statutes where none exist) to require that new surveillance applications must be approved by Congress. The strongest (and most difficult) form of approval would be to require an act of Congress in the form of a further amendment to the enabling statute. Short of that, formal approval of the relevant House and Senate authorizing committees could be required. Alternatively, agencies could be required to give the authorizing committees 60 to 90 or 120 days' formal advance notice, so that an investigation could be conducted and oversight hearings held, if desired.

As an alternative or complement to such congressional notice and/or approval options, OMB'S role could be strengthened by setting up a separate, statutory office within OMB and mandating a minimum staff. However, some of OMB'S other responsibilities may conflict, and it is unclear that such an office located in OMB would or could provide effective oversight. There is also the option of establishing agency staff in the data protection area and/or assigning new responsibilities to the Privacy Officers and/or Inspector General offices.